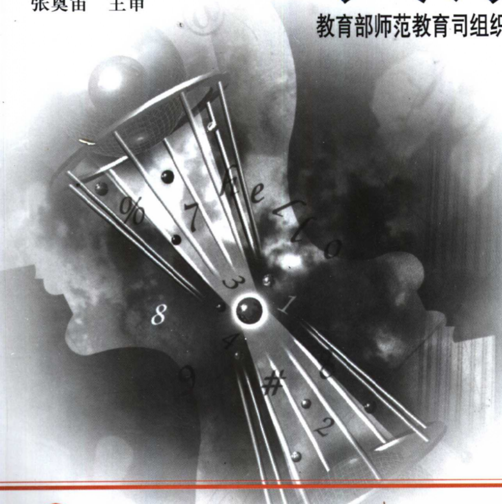
现代数学大观

赵小平　主编
张奠宙　主审

教育部师范教育司组织评审

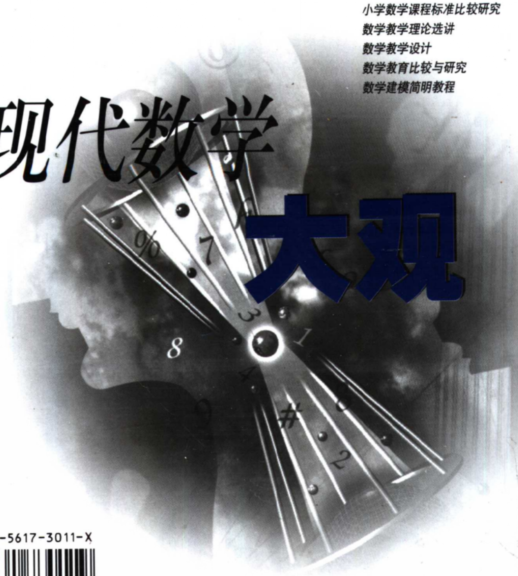


华东师范大学出版社

全　国　中　小　学　教　师　继　续　教　育

数学专业教材

现代数学大观



ISBN 7-5617-3011-X
9 787561 730119 >
O·126 定价：14.00元

现代数学大观

赵小平　主编
张奠宙　主审

华东师范大学出版社

图书在版编目(CIP)数据

现代数学大观/赵小平主编.一上海:华东师范大学出版社,2002.9

ISBN 7-5617-3011-X

Ⅰ.现… Ⅱ.赵… Ⅲ.高等数学-师资培训-教材 Ⅳ.O13

中国版本图书馆CIP数据核字(2002)第056950号

现代数学大观

主　　编　赵小平
责任编辑　宋维锋
封面设计　黄惠敏
版式设计　蒋　克

出版发行　华东师范大学出版社
市 场 部　电话 021-62865537
　　　　　　传真 021-62860410
http://www.ecnupress.com.cn
社　　址　上海市中山北路3663号
　　　　　　邮编 200062

照　　排　南京理工排版校对有限公司
印 刷 者　江苏昆山亭林印刷总厂
开　　本　890×1240　32开
印　　张　10.75
字　　数　283千字
版　　次　2002年9月第一版
印　　次　2002年9月第一次
印　　数　001-5100
书　　号　ISBN 7-5617-3011-X/O·126
定　　价　14.00元

出 版 人　朱杰人

(如发现本版图书有印订质量问题,请寄回本社市场部调换或电话021-62865537联系)

编者的话

本教材是华东师范大学数学系教师的集体创作，只有一个例外：北京师范大学的严士健教授。他为本书写了“鱼塘里有多少鱼——从超几何分布谈起”。一本教材为何要动员如此多的教授来完成，究竟难在何处？

本书创作的艰辛，一言难尽。首先是没有类似的著作可做参考，一切几乎都得从头做起。其次是现代数学内容广泛，一个人的知识范围有限，不得不集中大家的智慧。再次，更难的是通俗化。各门数学学科的专家有自己的一套语言、概念、定义、定理、公式，如果照此写下来，读者必定昏昏欲睡。因此，如何将朴素的原始数学思想以生动、平和的语言写出来，使读者得到现代数学观念的熏陶，是本书写作的最难之处。写成现在这个样子，已经花了九牛二虎之力，但是仍然不能说令人满意。

本书是中学数学骨干教师国家级培训的产物。《现代数学选讲》是一门必修课。本书就是该课的一份讲义。为中学教师写书，应是高师院校教师的责任，也是一份光荣。不过，许多中学教师似乎并不喜欢这门课，说是离开中学太远，适应不了教学需要。这有数学教师方面的原因，更多是这门课程内容上的问题。这份讲义，是在正反两方面经验的基础上完成的。教学效果逐步改进，最后受到了一定的欢迎。

中学数学教师不喜欢现代数学是一个老问题，也是个普遍的问题。这是数学的悲哀，也是数学教育的悲哀。君不见，中学物理课本里有爱因斯坦的相对论，化学教材里有“化学键”理论。生物学教师不懂“克隆”、DNA 和 RNA 的常识觉得说不过去，语文教师则和大

学教授一样地研究鲁迅、老舍、郭沫若，达到当代研究的前沿。为什么惟独中学数学和现代数学如此隔绝？

确实，数学有其严格的逻辑顺序，往往不是螺旋上升，而是“初等数学”、“高等数学”那样地直线安排。有人把它形容为“铁路警察，各管一段”。中学数学老师不懂现代数学，照样当特级教师。但是，特点只是特点而已，总不能脱离一般的科学规律。事实上，数学还有另外生动活泼的一面，数学的原始观念同样是朴素易懂的。现代数学和中学数学之间并没有不可逾越的鸿沟。数学的表述过于形式化，给人那种“枯燥”“干瘪”“难懂”的感觉，责任在数学家自己。过去，数学以女王自居，又不肯走下“王位”，“与民同乐”。但是，随着时代的改变，数学正在深入到各行各业，乃至千家万户。数学已经从幕后走到台前，以数学技术服务于社会，显示出“高效、优质”服务的“侍女”的一面。“女王”和“侍女”是数学的两个侧面，缺一不可。数学，是到了要改变自己公众形象的时候了。本书就是这样一种尝试。我们用尽量通俗的笔触，把现代数学若干侧面展现出来，力图给人一种易于接近、比较可亲的形象。

一些中学数学教师不喜欢现代数学，酿成这杯苦酒的还有高师院校自己。高师数学系的课程中，过度追求形式化成为一种遗传，一直带到中学。数学教学要讲推理，但更要讲道理；要讲究严格表述，也要提倡直观把握。物理学讲原子反应，大家均不知其详，却依然听得津津有味。惟独数学的规矩，要讲就“讲深讲透”，推导正确，证明完备。师范性要求中学数学教师如此束缚自己，事事都谨小慎微，不敢往前迈步，实在有点害人。例如，高师数学系课程中有“几何基础”、“数的概念”之类老前辈已经开拓好的平台，本来了解平台之后“大胆地往前走”就是了，偏偏只有高师数学系“谆谆告诫”说，这是“基本功”啊，“基础”啊，不学好将来危险啊（综合性大学数学系从来不开这些课，却没有任何危险）！难道师范院校只会往下看，往后看？多往前看看如何？于是我们设想这本《现代数学大观》，应该体现往前看的态度。“大观”的有些内容，不能深究，也只是“望望”而已。比如看一个建筑，可以观察内在细部结构或工艺技术；也可以是瞭望其

外部轮廓、欣赏其外在的美，求得总体把握。总之，许多数学也是可以“望一下”的。当然，严格推理和大胆想象，局部处理和宏观考察，二者需要有机结合，不能单打一。

时序到了2001年，新世纪开始了。数学教育呈现出新气象。国家中小学数学课程标准有了重大变化。微积分、矩阵向量、数据处理、算法分析、数学建模、数学文化，都会相继进入高中课程，再用老眼光看中学，“固守”初等数学，恐怕是不行了。高师数学系的面貌也在改变。数学建模、数学实验、数学教育概论、数学教育技术，包括“现代数学大观”等等课程，都会使未来的数学教师具有新的数学观念和数学知识结构。那时，中学数学教师懂一些现代数学，就是水到渠成的事。

最后，我们说说本书的结构。这里一共有三个部分：

第一部分，现代数学概貌。这是宏观地考察20世纪的数学和展望21世纪的数学。数学是社会的一部分，我们应当从社会进步的角度寻找数学发展的轨迹，不能只在数学内部的逻辑关系里兜圈子。

第二部分，现代数学基础专题选讲。它涉及一批基本的数学专题，从集合论开始，包括随机性数学、模糊性数学、数学结构、拓扑方法、算法分析、统计聚类、运筹优化、选举模型等等。主要是了解现代数学的基本思想和基本走向。读者可以借助一些例子，体会现代数学的真谛和价值。

第三部分，现代数学若干进展介绍。这一组问题涉及现代数学的重要事件和主要成就。包括编码和密码、时空几何、费马大定理的解决、小波分析、非线性数学、混沌、分形、金融数学等等。这些课题在一定程度上反映了当代数学的进展。尽管内容比较深奥，但叙述上强调深入浅出，读懂一个大概是必要和可能的。

本书称为“大观”，就是想让学生知其大意、观其轮廓、感受其深刻、欣赏其美丽，旨在扩大视野，提高修养。当然，这里并非只是空话，还是有真正的数学内容，至少是一些重要的范例和问题，还是要弄清其数学含义。

凡事开头难。我们希望通过这门课程的开设，有助于数学教师

数学观的转变，数学教育观的更新，以新的面貌，迎接21世纪的挑战。至于是否能够达到原有的设想，则需要由实践来检验，特别是中学教师的检验。我们期待着。

编审者

2001年9月

作者分工：

第一章　张奠宙

第二章　张奠宙 蒋鲁敏 赵小平 王继延 刘宗海 等

第三章　陈果良 王静龙 严士健 柴俊 袁震东 朱德明 沈纯理 陈志杰 等

前　言

数学，一种古老而又年轻的文化。人类从蛮荒时代的结绳计数，到如今用电子计算机指挥宇宙航行，无时无刻不受到数学的恩惠和影响。一个发达的社会，没有强盛的数学研究是不可想象的。

历史为我们作出了答复。古埃及尼罗河边的几何学为金字塔的辉煌催生。伴随古希腊文明出现的是《几何原本》。漫漫的中世纪长夜，欧洲数学归于沉寂。文艺复兴的来临，涌现出开普勒、笛卡儿、帕斯卡、费马这样的数学天才。17 世纪的伟大科学革命，始自牛顿——一位伟大的物理学家，也是一位数学家，微积分的发明者。拿破仑的凯旋，孕育了法国数学学派。大数学家高斯、黎曼、克莱因、希尔伯特，随着德意志资产阶级的兴盛而成长。当 1933 年希特勒葬送德国数学之后，世界数学中心移到美国的普林斯顿。改变人类生活的电子计算机，出现于 1940 年代的美国，它的设计人是一位数学家：冯·诺伊曼。

2000 年 8 月在日本东京举行国际数学教育大会，大会主席藤田宏教授提到数学发展史上的四个高峰：

公元前 300 年的欧几里得《几何原本》；

微积分的发明和应用；

19 世纪至 20 世纪初的公理化数学；

以计算机技术为基础的当代数学。

和第二个高峰相似，当代数学课题更多地来自现实需要，数学方法丰富多样，数学和其他科学的交互作用空前活跃。许多高新技术的本质可以归结为一种数学技术。而且，数学作为一种技术，可以直接产生经济效益。这就是说，数学已从社会发展的幕后走向台前。

一场悄悄的数学革命，正在我们身边发生。

● 变化着的数学观——从陈景润到王选

1970年代末期，中国的科学春天来临。徐迟的报告文学《哥德巴赫猜想》风靡全国，陈景润的名字一夜之间传遍大江南北，成为中国科学复兴的英雄。他在“哥德巴赫猜想”上的成就至今仍在世界上领先。当费马猜想于1995年宣布解决之后，21世纪的数学难题中，彻底解决“哥德巴赫猜想”成为数学家面临的主要课题。

陈景润从事的数论，是一门纯粹科学。数论的价值何在？一方面，在智力奥林匹克赛场上角逐，胜者为王。另一方面，世界顶尖数论专家纷纷投身密码研究，数论研究涉及国家安全以及企业机密。但是，中国的数学和公众之间存在着某种隔膜。尽管陈景润的科学精神感人至深，但是公众普遍认为，数学只是其他科学的语言，只能作为训练思维的体操。至于数学对经济建设的贡献、对社会的推动则是间接的，演不了主角，顶多是“幕后英雄”而已。

进入1990年代，情况逐渐发生变化，数学技术开始在中国显示威力。一项闻名中外的科学成就又一次和数学结缘：以王选为总裁的方正集团开发了“汉字激光照排系统印刷技术”。王选，1962年毕业于北京大学数学系。他所领导的这项告别“铅与火”的印刷术革命，其原理基于一项数学技术——“数据压缩”。目前，方正集团及其伙伴占领了汉字印刷国内市场的99%，国外市场的70%。王选成为中国“最能挣钱的科学家之一”。数学可以直接产生经济效益，又一次为事实所证明。数学对社会的贡献已从间接服务转变到直接干预，也就是说，数学的社会功能已从单纯为其他学科提供工具，发展为直接创造价值。

● 无处不在的数学技术——从CT扫描到飞行控制

在第二次世界大战期间，许多数学家进行了反对希特勒法西斯的努力，一大批直接服务于战争需要的数学技术随之产生。

1940年，英国和美国海军为了对付德国潜艇的威胁，创立了运筹学。在不增加设备的情况下，依靠数学智力，运筹学可以帮助提高设备能力和使用效率。

1942 年，苏联的柯尔莫哥洛夫和美国的维纳分别研究火炮的自动跟踪装置，发展随机过程的预测和滤波理论，提高防空效率。1948 年维纳发表著名的《控制论》。

1939 年起，英国的数学家图灵帮助英国情报部门破译德军密码成功。美军破译日军密码电报，击落日本大将山本五十六的座机。

1944 年，冯·诺伊曼创立的对策论用于太平洋战争的战术决策。

美国政府组织的“应用数学小组(AMP)”，参与空中火箭发射、水下弹道、B-52 轰炸机的计算等。数学家参与原子弹的研制。波兰裔数学家 S·乌拉姆为氢弹研制作出了关键贡献。

数学在反法西斯战争中卓有成效的工作，极大地改造了数学本身。战后和平时期的数学技术，基于计算机的应用在更广阔的范围内展开。

1950 年，冯·诺伊曼等使用电子计算机进行“数值”天气预报。他们使用计算机求解大气环流方程，迅速得出数学解，和经验预报相印证，获得成功。

计算机技术的迅猛发展，使得计算机模拟技术得以实现。飞机设计不必都在风洞中做实验，测试大炮性能不必都采用实弹射击，原子弹等地下核试验可以在计算机上模拟，甚至可以在计算机上进行军事演习。

1979 年的诺贝尔医学奖授予美国的柯马克和英国的洪斯费尔德，褒奖他们运用数学上的拉东变换原理，设计了 CT 层析仪。人体层析摄影技术造福千千万万的人群，说到底乃是一种数学技术的实现。

工业管理的自动化，除自动化设备之外，往往还有一项价值上百万的“说明书”，其实就是一个“数学模型”，一些数据而已。

人们享受数学文明可说无处不在。飞机起飞降落定位需要卡尔曼滤波技术，汽车设计需要计算机模拟，企业管理使用数学模型，医院看病使用数字技术，药品效果有赖统计分析，股票涨落需要数学估算，计算机设计使用 2 进位数，软件设计依赖离散数学，人工智能的

基础是数学方法……

在社会科学方面，人口预测、环境控制、保险精算、交通管理、社会发展模型，都离不开数学的参与。《红楼梦》作者是谁？统计学家作出了客观的判断。

1990年代以前，日本是电视大国。为研制高清晰度电视的制式，日本和西欧国家在模拟制式上投入了数十亿美元。但是，1993年美国的数字化电视方案出世后，立即“横扫千军”，使模拟式方案变成一张废纸。支持电视数字化的是一种数学技术——小波技术，它能将庞大的数据压缩到最低限度，使得图像的数字传输成为可能。这样，21世纪世界电视业的领导权也就落入美国手中。数学技术的威力，由此可见一斑。

有人预言，未来的数学研究，只有10%的工作以发表论文为目的，90%的数学将是到各行各业用计算机解决那里的数学问题。这种估计虽然有些言过其实，但作为一种发展趋势，恐怕不无道理。

● 金融数学异军突起——诺贝尔经济学奖中的数学工作

经济学中运用数学方法，在计划经济时代曾经不被重视。1938年，苏联著名数学家康特罗维奇创建“线性规划”方法，可以使线性约束条件下的线性目标达到最优。不过它在苏联长期未能推广。但是，美国独立发现的线性规划方法，每年可以为企业获得几十亿美元的经济效益。1971年，康特罗维奇和美国的柯普曼共同获得诺贝尔经济学奖。

西方的数理经济学已经有100多年的历史。其基本原理是一般经济均衡理论。一个经济体有生产者和消费者。消费者追求消费的最大效用，生产者追求生产的最大利润。价格杠杆对需求和供给进行调节，最终使市场达到一个理想的平衡。这套理论的理想研究方式是数学方法，特别是公理化方法。用数学工具得到理想均衡模型的经济学家，先后成为诺贝尔经济学奖获得者。其中有1970年的萨缪尔森，1972年的希克斯、阿罗，1983年的德布鲁。阿罗和德布鲁都是科班出身的数学家。

由于西方证券市场的发展，证券理论的研究和实践在经济学中

的地位日益突出，终于发生了“华尔街革命”。1990 年的诺贝尔经济学奖授予马克维奇、夏普和米勒。他们研究如何在多种证券上投资，能使收益最大。他们把收益和风险这些本来非常模糊的概念变成明确的数学概念，并导出资本资产定价模型等重要理论。1997 年的诺贝尔经济学奖则授予肖尔斯和默顿，他们的工作与期权定价理论有关。

期权，是指在未来某时刻以某种价格购买某货物的权利。比如，我们约定在明年 11 月 1 日，以每千克 1 元的价格收购 1 万千克的柑橘。如果那时的市价高于 1 元，则仍以 1 元收购。如果低于 1 元，则可以不收。这样的稳赚不赔的“期货购买权利”，当然要付出代价——期权的价格。1973 年，布赖克和肖尔斯提出了计算期权定价的公式，这是用随机微分方程、布朗运动、随机积分等数学工具描述的一个公式。由于数学计算结果和期权实际成交价格十分吻合，这一数学金融技术引起了华尔街的“金融革命”。布赖克于 1995 年去世，所以没有和肖尔斯一起获得 1997 年的诺贝尔经济学奖。

在 1990 年代末，国际金融危机屡屡发生。英国老牌的巴林银行因期权投机而倒闭。亚洲金融危机爆发。国际金融大鳄想吞噬香港没有成功。一些对冲基金由于忽视小概率事件遭到重创。这些震荡世界的金融事件，都是金融数学的研究对象。异军突起的金融数学现已引起国人的极大重视，我国数学家也在这方面有一些出色的工作。1997 年，国家自然科学基金会把金融数学列为优先发展的学科之一。

● 数学是统一的——“核心数学”更加“核心”

由于计算机技术的发展，20 世纪下半叶数学发展的一个大趋势是应用。但是，应用数学的基础是“核心数学”。没有核心数学的支持，数学应用是走不远的。历史一再证明，许多数学不能立刻应用于实际，却往往在不经意的时候获得应用。19 世纪高斯研究的数论，没想到会在 20 世纪的密码学中大显神威。非欧几何与张量分析是纯粹理性思维的产物，几十年后在爱因斯坦相对论中获得应用。拉东变换曾经是一个不起眼的纯理论，不想却为 CT 层析技术提供了

数学模型。三角级数是老学科了，数据压缩使用的小波技术正发生在这块土地上。陈省身在1940年代创建的纤维丛理论（整体微分几何），竟在1970年代的杨振宁-米尔斯规范场理论中得到解释。“数学有用”的不可思议性是我们认识数学的一项基本原则。

和数学应用一样，核心数学同样在飞速发展。“数学危机”“数学蒙难”只是某些哲学家在故作“惊人之语”。核心数学的发展趋势至少有以下特点：

第一，从线性到非线性。混沌、分形、动力系统等研究进展迅速。

第二，从交换到非交换。矩阵、算子的乘法都是不可交换的。

第三，从1维数学到高维数学，特别是4维和无穷维。

第四，随机数学和确定性数学、离散和连续、局部性质和整体性质间的对立与整合。

无论数学怎样发展，数学至今是统一的。由于中国过去的经济不够发达，数学课题不够前卫，数学观念不能迅速更新，才使得数学技术的价值没有在社会上、科学管理机构里，以及数学界自身得到充分认识。因此，近年来我国许多著名数学家大声疾呼数学应用的重要性。然而，发展数学技术决不是否定纯粹数学的价值。历史教训值得记取。应该说，“核心数学”更加“核心”，“应用数学”更加“应用”。我们所要做的只是数学的平衡发展。

2002年的国际数学家大会将在北京召开，这是中国数学进步的新起点。愿中国数学在新世纪里更上一层楼，实现“21世纪的数学大国”的理想。

目　录

第一章

现代数学概貌

第一节 数学科学的百年回顾

1900年,在巴黎举行的国际数学家大会上,数学大师D·希尔伯特(Hilbert, 1862—1943)在讲演的开始就说"揭开隐藏在未来之中的面纱,探索未来世纪的前景,谁不兴奋呢?"[1]接着,他提出了20世纪需要解决的23个数学问题。现在,20世纪已经过去,一百年来,数学面纱一层层被揭开。爱因斯坦的相对论,20年代出现的量子力学,产生于50年代的杨-米尔斯规范场论,使微分几何、拓扑理论、抽象分析获得全新的原动力。电子计算机的出现,改变了人类社会的生活方式,也改变了数学本身。数学技术渗入到航天飞行、医疗检测、经济管理以及众多的社会科学领域。在20世纪末,费马猜想终于获得证明,成为人类智慧的一种最高象征。希尔伯特在1900年提出的问题,多半已经有了结果。今天,数学家们又在为21世纪的数学问题进行构想。数学科学仍将一日千里地迅速发展,在探索自然奥秘和推动社会发展中作出自己的贡献。中国数学应该在新世纪为人类作出更大的贡献。

1. 20世纪数学的开端(1900—1918)

在19、20世纪之交,法国的H·庞加莱(Poincare, 1854—1912)是无可争辩的数学领袖。他在三体问题、微分方程的定性理论、拓扑学的大量原创性研究,成为挖掘不尽的数学宝藏。如果说庞加莱主要以自然科学的实践背景为数学研究的源泉,那么德国的希尔伯特则更多地从数学本身的完善上寻求数学的进步。他的著名工作有数论报告、几何基础、抽象积分方程与抽象空间。希尔伯特倡导

的形式主义学派，成为 20 世纪的主导数学哲学。

这一时期最重要的数学事件，是爱因斯坦的相对论把新时代的几何学推到了科学的最前沿。四维时空的狭义相对论，产生了闵可夫斯基空间几何。弯曲时空的广义相对论，使得张量分析、黎曼几何、高维几何成为物理学革命的工具。我们生存着的宇宙空间，可以用黎曼在 1867 年创立的高维流形和曲率理论来描述。人们不禁惊叹造化之工，数学之巧。

在物理学推动数学发展的同时，纯粹数学也以惊人的方式大步前进。19 世纪初，J·B·傅里叶(Fourier, 1768—1830)提出的调和分析，是众多数学分支的出发点。G·康托尔(Cantor, 1845—1918)从研究傅里叶级数的唯一性提出“点集”的概念，以后发展为“集合论”，成为所有抽象数学的表述工具。法国的 H·勒贝格(Lesbegues, 1875—1941)创立了建立在可列可加测度上的积分理论，使得许多黎曼意义下不可积的函数也可以进行傅里叶展开，实现了一次积分革命。康托尔和勒贝格建立的数学理论，常常涉及一些没有导数的病态函数、没有切线的奇异曲线，以及看上去千疮百孔的怪异集合。当时的数学家难以想像勒贝格积分竟会成为 20 世纪工程师手中的工具。

康托尔的集合论是一个怪物，他所建立的关于无限集合的超限数理论很难使人接受。例如，正方形一边上的点和对角线上的点一样多。康托尔本人也陷入了自己提出的一个悖论：由一切基数(cardin number)构成的集合 S，其基数将大于 S 中的所有基数。这使康托尔日夜难寐。当时德国数学界的当权人物克罗内克(Kronecker, 1823—1891)曾对康托尔的无限观进行猛烈的抨击，反对康托尔进入柏林大学。康托尔于 1884 年患精神分裂症，病情时好时坏，1918 年病逝于哈雷精神病研究所内。希尔伯特是康托尔数学业绩的积极支持者。他曾说：“没有人能把我们从康托尔所创造的天国中赶走。”[2]

1903 年，英国哲学家、数理逻辑学家 B·罗素(Russell, 1872—1970)发现了一个十分简单的悖论：考察一切不以自身为其中一元素的集合所构成的集合 B，此时若 $x \in B$，则有 $x \notin B$；而若 $x \notin B$，则

又有 $x \in B$，横竖都不对。这触发了数学基础的大论战，史称“第三次数学危机”。为避免罗素悖论，罗素提倡“逻辑主义”，认为数学即逻辑，只要数理逻辑没有矛盾，数学就不会有矛盾，而且是永远绝对正确。希尔伯特则提出“形式主义”，认为数学研究的对象可以不必考虑实际意义，无非是一些对象按一套公理作形式演绎的结果。只要公理无矛盾、独立、完备，数学就永远绝对正确。直觉主义则采取保守态度，不承认“自然数全体所成的集合”，反对使用排中律，主张“数学对象的存在，必须能够构造”，因而把数学限制在很小的范围内。逻辑主义想把数学划归为逻辑的愿望未能实现，但留下了“数理逻辑”这门重要的学科。希尔伯特的形式主义后来被 K · 哥德尔(Godel, 1906—1978)的两个不完备定理所否定，寻求数学绝对严格基础的理想随之破灭。但是，形式主义的思想为后来的布尔巴基学派所继承和发展，对 20 世纪数学观念的影响极为深刻。直觉主义的思想过于保守，束缚了数学家的手脚，也没有得到广泛承认。只有构造主义的想法，随着电子计算机的出现，获得了新的生命力。

20 世纪初，英国的分析学派非常强大。G · 哈代(Hardy, 1877—1947)和李特伍德(Littlewood, 1885—1977)是领袖人物。他们在一个时期中的解析数论、单复分析、不等式、级数等在“硬”分析领域里有很高建树。哈代发现并培养了印度传奇数学家拉马努詹(Ramanujan, 1887—1920)。拉马努詹未受过正规教育，在不知道什么是现代意义下的严格证明的前提下，完成了大量的数学工作。拉马努詹的笔记本，写满了大量公式，但没有详细的证明。60 多年之后，美国的 B · C · Berndt 把拉马努詹笔记本加以整理，完成证明，分三册出版[3]。该书的研究表明，除少量公式有误之外，拉马努詹笔记本中的绝大部分是正确的。拉马努詹是如何进行数学思考的？这一数学之谜，仍有待解开。

经典的数学应用工作，仍在深入进行。力学、电学、光学、机械工程、建筑工程中的数学问题被大量研究。引人瞩目的工作是数理统计学以“生物统计学”的形式开始出现。标准差、平均差、相关等术语，在 1901 年由 K · 皮尔逊(Pearson, 1857—1936)创办的《生物计

量学》(Biometrika)杂志上陆续使用。

2. 以哥丁根学派为中心的黄金时期(1918—1933)

从第一次世界大战结束,到1933年希特勒法西斯上台,世界的数学中心在德国的哥丁根大学。在哥丁根学派的带动下,出现了20世纪数学发展的一段黄金时期。

哥丁根是德国的一座小城,以哥丁根大学而著名。大数学家高斯(Gauss, 1777—1850)曾长期在此工作。1886年,F·克莱因(Klein, 1849—1925)来哥丁根任教授并主持数学系,遂延请希尔伯特、闵可夫斯基来校执教,不久就成世界数学中心。第一次世界大战结束时,德国虽是战败国,但数学的元气未伤。法国在大战中损失了一代大学生,巴黎高师的学生名册上布满了黑框。在20世纪20年代,法国几乎是函数论王国,很少有新学科产生。一个例外是E·嘉当(Cartan, 1869—1951),他在李群表示、外微分方法、活动标架法、微分方程组的研究上有独到的见解,成为日后微分几何的经典性工作,可惜当时未受到充分重视。英国继续维持哈代的分析学派,没有新的突破。20世纪20年代的美国数学,还远远落后于西欧。前苏联、东欧诸国的数学刚刚起步。尽管优秀数学家遍布欧洲和世界各地,哥丁根却是公认的世界数学中心。

在20世纪20年代,克莱因已经退休,希尔伯特也已老了。闵可夫斯基则因病在1909年去世。但是,新人在不断成长。希尔伯特的继承人是H·外尔(Weyl, 1885—1955)。他是全才的数学大家,他创立的学科数不胜数,例如,数论中的一致分布理论、黎曼曲面、微分流形、算子谱论、偏微分方程、胞腔概念、规范场理论、李群表示、数学物理等等,都在他的手中得到改观。

克莱因的继承者是R·柯朗(Courant, 1888—1971)。他专长分析,在数学物理方程、差分方法、变分学等领域都有创造性的工作,尤其具有行政组织能力;1929年,柯朗任哥丁根数学研究所所长。20世纪最伟大的女数学家E·诺特(Noether, 1882—1935)在哥丁

根完成一般理想论，创立了抽象代数学科。

冯·诺伊曼曾是希尔伯特在数学基础研究上的助手。

20世纪20年代，前苏联数学学派开始崛起，鲁金（Lusin, 1883—1950）和叶戈洛夫（Egorov, 1869—1931）领导的函数论群体，出现了像柯尔莫哥洛夫（Kolmogorov, 1903—1987）、亚历山大罗夫（Alexandrov, 1896—1982）那样著名的数学家。他们都和哥丁根有密切联系。柯尔莫哥洛夫常到哥丁根访问，他的成名作《概率论的基本概念》[4]，用测度论和实变函数论方法，把概率论建立在完全严格的基础上。此书最初是用德文写成并发表的。亚历山大罗夫则和诺特联系密切。诺特对亚历山大罗夫建立代数拓扑学有关键性的建议。第一次世界大战之后，波兰数学发展迅速。这一学派的中坚人物，如西尔宾斯基（Sierpinski, 1882—1969）、斯坦因豪斯（Steinhauss, 1887—1972）都深受哥丁根学派的影响。

在20世纪20年代，量子力学的诞生，是物理学的又一场革命。哥丁根学派及时为量子力学提供了数学框架。冯·诺伊曼的《量子力学的数学基础》，外尔的《群论与量子力学》成为一个时期的经典著作。[5]

这一时期数学成就的特色是：无限维空间、抽象的代数方法、几何上的大范围整体性质，显示出与19世纪的数学在研究对象和研究方法上有了根本的差别，而以三个数学新分支的形成为重要标志：

(1) 泛函分析

它起源于希尔伯特的抽象积分方程理论，其中使用了由无限维正交系所生成的完备空间，现在称之为希尔伯特空间。冯·诺伊曼正是利用这一理论为量子力学提供了数学框架（1929年）。此外，波兰的S·巴拿赫（Banach, 1892—1945）提出了赋范空间，发展了其上的算子理论。

(2) 抽象代数

以诺特于1926年发表的一般理想论为主要标志。在汉堡大学的E·阿廷（Artin, 1898—1962）也做出了开创性的工作。范·德·瓦尔登（Van. der Waerden, 1903—　）于1932年出版的《代数学》

是抽象代数早期工作的总结。

(3) 拓扑学

其基本思想可导源于庞加莱于 1896 年所写的《位置分析》。由于康托集合论的影响,研究数列和函数各种收敛性的点集拓扑学随之产生,其代表作是德国数学家豪斯多夫(Haussdorf, 1868—1942)于 1913 年完成的《集论纲要》。但是,意义更为重大的几何拓扑学由苏联的亚历山大罗夫和瑞士的 H·霍普夫(Hopf, 1894—1971)合作完成。他们合写的《拓扑学》(1935 年)是拓扑学最早的经典著作。与此同时,美国的 S·莱夫谢兹(Lefchetz, 1884—1972), J·W·亚历山大(Alexander, 1888—1971)和 H·M·莫尔斯(Morse, 1892—1977)分别以拓扑不动点理论,曲面同调论和临界点理论为拓扑学增色。在 20 世纪 20 年代的美国,拓扑学的研究是在世界上领先的少数学科之一。1930 年,比利时的德·拉姆(De·Rham, 1903—1969)给出高维微分流形上微分形式和上同调性质的关系,是一项重要的成就。

1933 年,柏林大学、哥丁根大学等德国一流大学的校园内贴出告示,让一切犹太人离开学校。德国数学就此被断送。

3. 反法西斯战争时期的数学(1933—1945)

1930 年以后,德国政局动荡,法西斯的阴影笼罩欧洲。冯·诺伊曼首先觉察到未来的变化,于 1930 年到了美国的普林斯顿大学。此时,美国企业家资助成立的普林斯顿高等研究院刚刚成立。1933 年之后,研究院首批聘请的 6 位研究教授是爱因斯坦、外尔、冯·诺伊曼,以及美国数学家 J·W·亚历山大,H·M·莫尔斯和研究工作的组织者 O·维布仑(Veblen, 1880—1960)。这份名单预示着普林斯顿将是未来的世界数学中心。同时到达美国的有柯朗、E·诺特、阿廷,数学基础方面的天才 K·哥德尔,概率论专家 W·费勒(Feller),分析学家 G·波利亚(Polya)和 G·切戈(Szego)等等。那时美国正值经济大萧条时期,大学的经费相当困难,在维布仑等的努

力下,美国容纳了这批精英人士,使美国数学迅速达到世界的顶峰。与此对照,德国数学一蹶不振。L·比贝巴赫(Bieberbach, 1886—1982)因提倡“日耳曼数学”而臭名昭著,富有数学才华的泰希穆勒(Teichmuller, 1913—1943)忠于希特勒而死于战场。

数学家们积极投入反法西斯战争,并促进了数学的发展。

1940年,英国和美国海军为了对付德国的潜艇威胁,发展了运筹学。这种旨在提高设备能力和使用效率的学问,战后大量用于经济部门。1938年,苏联的L·康特罗维奇(Kantolovic, 1912—1986)发明线性规划的单纯形解法。战后美国的但泽(Dantzig, 1914—)独立发现了该法,并在经济部门推广使用,有极高经济效益。

1942年,苏联的柯尔莫哥洛夫和美国的N·维纳(Wiener, 1894—1964)分别研究火炮的自动跟踪,形成随机过程的预测和滤波理论。1948年,维纳写成《控制论》一书,开辟了新的学科。

1939年开始,英国数学家A·图灵(Tmring, 1912—1954)帮助英国情报部门破译德军密码成功。

1944年,冯·诺伊曼发展对策论,并用于太平洋海战。美国政府组织的AMP (Applied Mathematics Panel,应用数学小组),吸收了大批数学家参与工作。柯朗和他的助手研究喷气式飞机,水下爆炸。代数拓扑学家惠特尼(Whitney, 1907—1989)曾研究空中发射火箭。G·伯克霍夫(Birkhoff, 1912—)负责考察水下弹道学问题。代数学家S·麦克莱因(Maclane, 1909—)曾是AMP的技术代表。统计学家沃尔德(Wald, 1902—1950)为节约实弹射击试验的弹药而提出“序贯分析”方法。出生于波兰的数学家S·M·乌拉姆(Ulam, 1909—1984)参加原子弹的研制,并在计算和估计中发挥了关键作用。数学家的这些努力,对于提高数学在国家和公众心目中的地位,有十分重要的作用。

在应用数学迅猛发展的同时,纯粹数学也在继续前进。最引人瞩目的是法国的布尔巴基学派。当德国数学衰落之时,以J·迪厄多内(Diendonne), A·维伊(Wiel)为代表的一批法国年轻数学家,冲破“函数论王国”的束缚,力图以结构主义的观点整理全部数学,

1939 年出版《数学原本》第一卷[6]。他们的观点在第二次世界大战之后影响巨大。

拓扑学继续迅猛发展。同伦论和同调论取得长足进步。分析学继续是数学的主体,但是代数学、微分几何学正在成为现代数学的主流学科。此时最重要的结果有:O · 扎里斯基(Zariski, 1899—1986)将意大利学派的代数几何学严格化;陈省身于 1945 年证明高维的高斯-博内公式,完成大范围微分几何的奠基工作;L · 施瓦茨(Schwarz, 1915—)提出广义函数论;冯 · 诺伊曼、I · M · 盖尔范德创建的算子代数和赋范环论;庞特里雅金发展"连续群论";英国的哈代,苏联的维诺格拉多夫,中国的华罗庚继续在解析数论上创造新的成果;费勒,柯尔莫哥洛夫,辛钦等建立的随机过程理论,冯 · 诺伊曼和乌拉姆创立的蒙特卡洛方法,在理论和实践上都有重大意义。

第二次世界大战期间的科学成果中,对数学影响最大的,当然是电子计算机的产生。冯 · 诺伊曼在这一影响人类历史进程的工作中起了关键的作用。

4. 美苏冷战时期的数学争雄(1945—1980)

第二次世界大战结束之后,美国和苏联分别代表西方和东方国家集团,进入了长达几十年的冷战时期。自 20 世纪 80 年代苏联进入戈尔巴乔夫时期后,冷战渐渐淡化,形成世界多极的态势。从数学上看,战后的几十年,也是美苏争雄的局面。普林斯顿高等研究院和莫斯科大学始终是世界两大数学中心。

五六十年代,是战后的恢复发展期。义务教育的普及,高等教育的大发展,为数学家们造就了极好的就业局面。数学家的人数大量增加,数学论文的数目呈爆炸之势,新的数学学科层出不穷。人们感叹,在冯 · 诺伊曼和外尔于 20 世纪 50 年代先后去世之后,能够总揽数学全局的数学家,似乎已经不会再有了。只有 1987 年去世的柯尔莫哥洛夫也许是一个例外。

尽管文献浩如烟海,重要的数学工作仍然十分令人注目。[7]这里

选取 9 项，当然是一些不完整的罗列：

- 连续群的解析性。即每一个局部欧氏群一定是李群。这一希尔伯特第五问题于 1952 年获得完全解决。
- 丢番图方程是可解的。在美国女数学家 J·罗宾逊工作的基础上，1970 年由苏联的马蒂塞维奇(Matiasevich)解决了这一希尔伯特第十问题。
- 阿蒂亚(Atiyah)-辛格(Singer)指标定理。这是将一般流形的拓扑结构和其上微分算子的核空间维数联系起来的深刻结果。(1963 年)
- 动力系统的 KAM 定理。由柯尔莫哥洛夫、阿诺尔德(Arnold)、莫瑟尔(Moser)三人的工作所构成。现已成为三体问题，哈密顿系统研究的经典成果。(1954 年，1963 年)
- 大范围微分几何成为表述规范场论的数学工具。这是陈省身和杨振宁分别从数学和物理学上所得成果的统一。(1975 年)
- 有限单群分类的完全解决。(1980 年)
- 在八维空间中有一个流形，和七维空间中的单位球面同胚但不微分同胚，即所谓米尔诺(Milnor)怪球。(1956 年)
- 四色问题的电子计算机证明。1978 年由美国 W·黑肯(Haken)等在伊利诺伊大学完成。
- 选择公理和 ZF 公理体系独立。1963 年由 P·柯亨(Cohe)得到。

战后数学上最大的变化是电子计算机的使用。数学由此变成了一种技术——数学技术。科学计算成为继理论构建，实验考察之后的第三种科学研究方法。军事指挥，飞机设计，原子弹爆炸实验，化学反应，人口计划，气象预测，卫星定位，石油勘探，企业管理，一切都可以运用数学模型在计算机上进行。数学为人类创造了巨大的财富，节约了无数的资源，这一切很少被公众所充分了解。以数学工作获得诺贝尔经济学奖却已是十分常见的事情。

在这基础上，许多纯粹数学得到料想不到的应用。有限域和密

码学，数论和近似计算，纤维丛理论和规范场，拉东变换和 CT 扫描，拓扑学用于 DNA 分子结构。同时，由于计算机科学和人工智能的需要，组合数学得到了迅猛的发展。计算复杂性形成了一门艰深的理论。寻求多项式算法成为数学家注意的焦点。1979 年苏联哈奇扬(Hachijan)提出线性规划的椭球算法，以及后来的卡玛卡(Kamarka)算法都是轰动一时的新闻。起源于实际，却又大胆创新的学科相继涌现，如模糊数学、非标准分析、突变理论。它们的创立者都认为自己的工作是数学的一场革命，但这需要时间的检验。

总之，第二次世界大战以后，数学向科学"女王"和科学"侍女"两极发展。一方面，纯粹数学继续向高、深、难的方向进军，范畴、流形、纤维丛、多复分析、代数簇、上同调、鞅、分枝等新领域不断开拓。数学研究的对象从低维空间发展到高维空间以至无限维空间，函数和方程的研究从单变量发展到多变量，已经大体完成了的线性数学走向非线性数学，确定性数学和随机现象的数学彼此融合和渗透。纯粹数学仍然保持着至高无上，完全正确的华贵形象。另一方面，数学又极力为其他科学服务，为人类的生活服务，走近常人的生活，使得应用数学广泛渗入到各门学科中去，包括社会科学，科学数量化的进程可以说无孔不入，数学确已成为人们忠实的科学"侍女"。

5. 数学多极化时代来临(1980 年至今)

进入 1980 年年代，世界的政治经济出现多元化的格局。数学也不例外。一个大体的描述是：美苏继续领先，西欧紧随其后，日本正在迎头追赶，中国和其他地区正在迅速发展。1991 年苏联解体使其数学有所削弱，但独联体特别是俄罗斯的数学基础和研究实力仍然十分强劲，不可低估。

经过第二次世界大战以后的发展，数学家队伍有了空前的扩大，数学工作市场有饱和的迹象。纯粹数学研究仍会保持前进的态势，但要求有更高的研究水平，产生更有意义的成果。一些"无病呻吟"、"滥竽充数"的数学论文将会受到冷落，优胜劣汰的法则已经比过去

更加严厉地在数学界通行。这期间一个最激动人心的事件是费马大定理的证明。1983 年,德国的法尔廷斯(Faltings)证明费马定理如果有解,至多为有限个。1995 年,英国的怀尔斯(Wiles)在前人工作的基础上最终证明费马大定理是正确的。这是人类智慧的伟大象征,也是 20 世纪末一项最高的数学成就。

数学家大批转向计算机科学和人工智能领域,乃是就业市场自然调整的结果。同时,数学家利用计算机的威力,扩大和延伸了数学家的脑和手。非线性数学的发展得益于此。80 年代以来,混沌理论、分形几何、孤立子解、小波分析等数学热点,没有不和计算机发生联系的。

数学和物理学层面的交融,仍然是数学发展的重大源泉。1987 年,英国的唐纳森(Donaldson),在杨-米尔斯方程的求解过程中,发现四维空间中有一种流形,具有两种不同的微分结构,大出人们的意料之外。物理学家威顿(Witten)用物理学方法推演数学问题,虽然没有严格证明,却得到了正确的数学结果。希尔伯特的形式主义数学哲学,布尔巴基的结构主义数学观,在威顿的工作面前,显得无能为力。数学中经验主义是否正在复兴,只有猜想没有证明的"理论数学"是否允许存在的问题[8],正严肃地摆在数学界的面前。

6. 20 世纪的中国现代数学

中国的现代数学的开端可以追溯到徐光启(1562—1633)和利玛窦(R. Matteo, 1552—1610)于 1607 年翻译出版欧几里得的《几何原本》。清康熙帝玄烨曾经热心学过一些西方数学,此后少人问津。清末李善兰(1811—1882)曾和伟烈亚力(W. Alexander, 1815—1887)合译美国数学教材《代微积拾级》(1859 年)。李善兰恒等式至今犹有价值。1898 年京师大学堂成立,先后派遣一些学生到日本学习数学。其中有冯祖荀(1880—1943),后来长期担任北京大学数学系主任。清末到美国学习数学的胡敦复(1886—1978),郑桐荪(1887—1963),秦汾(1887—1971)起过一些先驱作用。1909—1911 年的三

年中。因美国退回部分庚子赔款而选送三批中国留学生到美国留学。以学习数学而著称的有胡明复(1891—1927),他于1917年在哈佛大学获得博士学位——中国第一位数学博士。姜立夫(1890—1978)于1911年到美国,1918年也在哈佛大学获得博士学位。与此同时或稍后,何鲁(1894—1973)与熊庆来(1893—1969)到欧洲研习数学。他们回国后推动了中国各大学数学系的创办,确立了中国现代数学的基础。

30年代的清华大学数学系实力雄厚。特别是陈省身(1911—)和华罗庚(1910—1985)两位青年学者的到来,使中国数学开始走向世界。江泽涵(1902—)致力于北京大学数学系的发展。从日本回来的陈建功(1893—1971)和苏步青(1902—)建设浙江大学数学系,使之成为中国数学发展的又一基地。到了抗日战争时期,西南联合大学已拥有陈省身、华罗庚、许宝騄(1910—1970)这样具有很高声誉的数学家,中国现代数学开始接近世界先进水平。

1949年之后,中国数学界的规模迅速扩大,数学门类逐渐齐全,并能够为国民经济和国防事业服务。华罗庚和吴文俊(1919—)等大批旅外数学家回国。陈景润(1933—1996)等年轻数学家成长很快,出现了一批在现代数学研究上卓有贡献的中国数学家,他们先后当选为中国科学院院士。1966年开始的"十年动乱",使中国数学前进的势头锐减,以至瘫痪。80年代以来,经过恢复时期,新一代的数学家成长起来。从1986年开始,中国数学家吴文俊、田刚、林芳华、张恭庆、马志明、励建书、李俊等先后应邀在国际数学家大会上作45分钟报告。后来被聘为中国科学院外籍院士的陈省身获沃尔夫奖,丘成桐(1949—)获菲尔兹奖,使中国数学界受到鼓舞。"21世纪数学大国"是中国数学界的共同愿望,经过几代人的不懈努力,这一理想正在逐步变为现实。

展望未来,我们需要总结过去百年世界数学走过的道路。纯粹数学研究中的原创性,开辟新学科新方向的意识和能力,以及在各行各业中数学意识的增强,克服国内应用数学发展的不平衡,也许是中国数学面临的严峻挑战。

参考文献

[1] D·希尔伯特. 数学史译文集. 上海科学技术出版社, 1981.

[2] M·Klein. 古今数学思想. 上海科学技术出版社, 1981.

[3] B. C. Berndt. Ramanujan's Note Books. Ⅰ, Ⅱ, Ⅲ, Springer-Verlag, 1985—1991.

[4] A. N. Kolmogorov. Grundbegriffe der Wahrsherinlich keitsrechung, Springer. 1932.

[5] J. von Neumann. Mathematische Grundlagen der Quantenmechnik. Springer, 1932.

H. Weyl. Gruppen Theorie and Quantenmechnik, S. Hirzel, Leipzig. 1928.

[6] N. Bourbaki. Element de mathematique, Livre I. Actual, Scient, Etinbuster, 1939.

[7] J·H·尤因等. 1940 年以来的美国数学. 美国数学月刊, Vol. 83. No. 7. 1976.

(中译本:世界科学译丛, 第一辑, 1979.)

[8] A. Jaffe and F. Quinn, Theoretcal Mathematics: Toward a culture synthesis of mathematics theoretcal physics, Bull Amer Soc, 29(1993) 11—13.

第二节 展望数学的明天

常常听说的“第三次数学危机”，不过是哲学家在研究数学大厦基础时所作的“惊人之笔”。其实，数学在一日千里地发展，甚至让你头晕目眩。大约从20世纪下半叶开始，数学进入新的高峰。数学观也随之发生改变。作为一名数学教师，如果不能对现代数学的发展有比较清醒的认识，其数学教学就会迷失方向。

2000年8月，国际数学教育大会在东京召开。大会主席、日本著名数学家藤田宏在大会报告中指出，迄今为止的数学，经历了四个高峰：

- 以欧几里得《几何原本》为代表的古希腊公理化数学。
- 以牛顿发明微积分为开端的无穷小算法数学。
- 以希尔伯特为代表的形式主义数学。
- 以计算机技术为代表的信息时代数学。

信息时代的数学已经来临了，我们的教学思想是否跟得上时代呢？

当然，展望未来是一件危险的事情，往往十说九不准。我们还是从现在开始，先来认识数学，认识数学的今天。

数学是什么？好像很清楚，又觉得不大清楚。从古以来，人们受教育的最低要求就是“会写信，会算账，不做睁眼瞎”。这算账便是数学。进入20世纪以后，全世界的基础教育都以母语和数学为两门最重要的课程。数学的内容除算术之外，还有代数、几何和三角。我国规定的九年制义务教育中，数学课年年有，还要年年考。这样说来，人们应该很了解数学才是。但是，尽管数学课这样多，人们却总觉得数学离自己很远，很神秘，数学很难学，数学没有用……。这有两方

面的原因，首先是数学本身的特点，它所具有的形式化抽象特征，使学生难以从现实生活中找到它的原型；另一方面，我国数学教育观上的偏颇，加重了数学远离现实的印象，造成了更多的误解。

因此，我们在探讨数学的明天时，先要从“什么是数学”这样的基本问题开始。

1. 数学在公众中的形象

数学是人类活动的结果，具有明显的社会性。从科学史家的眼光来看，人类社会的每一次重大进步，都伴随着思想革命，而数学的变革是其中主要的标志之一。奴隶社会阶段，古希腊文明是集中代表，以逻辑演绎为特征的希腊数学灿烂辉煌，集大成的《几何原本》对人类的影响至今不衰。近代的资本主义文明，以牛顿的万有引力学说为标志，由此产生的微积分勇敢地跨过了“无限”的门槛，可说是人类思辨能力的高峰。法国大革命带来了伟大的法国数学学派。20世纪最伟大的科学革命——爱因斯坦的相对论，是在黎曼几何的基础上建立起来的。伟大的数学家冯·诺伊曼成为计算机科学的奠基人，它的影响已经超越了数学学科本身，也超越了电子计算机本身，成为人类进入信息时代的象征。

数学的价值也逐渐为政府所了解。1998 年美国用于数学的预算达到 1 亿 8 千万美元，其中美国自然科学基金会的资助为 9 700 万美元，约占每年全部自然科学基金总额的 4%。据新财政年度的预算，数学方面的基金总额将增至 1 亿 9 千 5 百万美元。我国每年用于数学的资助额度缺乏资料，可以统计的是中国自然科学基金会对数学的支持，从 1986 年的 100 万增加到 1998 年的 2 千 4 百万，12 年间增长了 24 倍。

但是数学科学的价值并不能直接从日常生活，生产技术，经济发展中立刻体现出来，而要经过一个漫长的过程。所以，数学和公众之间存在着一层隔膜。著名的例子是诺贝尔科学奖中没有设立数学奖。在诺贝尔奖桂冠日益受传媒重视的时候，数学失去了宝贵的一

份。诺贝尔为什么没设数学奖？过去有许多猜测，如诺贝尔和某数学家交恶，设奖将会使该数学家得奖等等，但经瑞典皇家科学院调查，此说完全是子虚乌有。一个可以接受的理由便是，在诺贝尔看来，数学不是科学，只是人的一种智力活动，并不和自然界的现象发生直接联系。瑞典皇家科学院为了补救诺贝尔数学奖的缺失，于1982 年设立了与诺贝尔奖相同的克雷福德奖，授予诺贝尔奖未包括的 6 个领域，其中包括数学，每年颁授一个学科，所以数学每 6 年轮到一次。不过，它的影响远不能和诺贝尔奖相比。

1995 年底，美国纽约州的罗彻斯特大学闹出了一场数学风波。这所老资格的美国名牌大学的校长宣布，从 1996 年开始，停止该校培养数学博士生的计划(强项是代数拓扑学)。理由是办学经费紧张，而数学对学校的贡献很小，关闭数学博士培养项目，将不会影响其他系科的发展。这件事引起了美国数学界的强烈反应。经过调解斡旋，罗彻斯特大学的数学博士培养计划是保留了，但是数学过分脱离现实的状况，需要引起重视，而向公众宣传数学价值的任务也突现出来了。

改善数学在公众中的形象，是国际数学组织十分关注的事情。1992 年 5 月，在巴西里约热内卢的一次会议上，当时的国际数学家联盟(IMU)主席，法国数学家里翁斯(J. L. Lions)，以联盟的名义，宣告 2000 年为世界数学年(World Mathematical Year 2000)，简称 WMY 2000。这项计划得到联合国教科文组织和第三世界科学院的支持。它的一个重要目标就是“树立数学的形象”，即向“信息社会”系统地表现数学的价值，向大多数人显示数学科学上的精确的范例及应用；宣传数学在文化及社会中的作用；纵览数学对技术的影响；削弱公众中对数学的错误印象。

WMY 2000 的活动正在世界各地蓬勃展开，到 2000 年，有许多数学活动在世界范围内进行。中国数学会已经进行了准备工作。

1995 年，国际数学教育委员会秘书长尼斯(M. Niss)发表谈话建议：

2000 世界数学年的主要任务应是：“使数学及其对世界的意义

被社会所了解，特别是被普通大众所了解”。我们的主要目的不是宣扬数学的奇迹，游说与宣扬不仅不能使我们的听众信服，而且可能起反作用。相反，我们的任务应是揭示数学的五个本质：

- 作为一门纯粹科学。
- 作为一门应用科学。
- 作为决策与行动的工具。
- 作为一门艺术。
- 作为现代教育最重要的学科之一。

在中国，数学的社会形象还是比较好的。如果说国外的数学家是很少受到新闻媒介关注，相比之下，中国的情形则要好得多。传奇数学家华罗庚的事迹在生前就被拍成电视剧放映，可说在世上绝无仅有，他的名字已成为“天才，勤奋，聪明”的同义词，华罗庚曾任全国人民代表大会常务委员会委员；苏步青曾担任过全国政治协商委员会的副主席。数学家的社会地位之高，在其他国家相当少见。更令人瞩目的是徐迟的报告文学“哥德巴赫猜想”的成功轰动。数论，哥德巴赫猜想，“1＋2”，陈景润，一时间传遍大江南北。在那特殊的年代里，陈景润受到民族英雄般的传颂，被青年人看做科学的象征。数学被青年人视为皇冠上的宝石，从事数学研究成了一项崇高的事业。各高校数学系录取了许多资质优异的学生。80 年代中国数学青年中人才辈出，和“哥德巴赫猜想”的影响是分不开的。不过，徐迟的这篇报告文学在成功的同时，却也带来一些负面的影响。似乎数学家都得象陈景润那样的穷苦、偏执、与世隔绝，而且万般无奈，才会成功。其实，数学家也是普通人，一样食人间烟火的。

另一方面，数学的形象有时也不太好。在一些名人笔下，说到自己小时候“数学学不好”的时候，一点也不脸红，似乎还有点“洋洋自得”的味道。据报导，中国学校里成绩不好的学生，主要是数学成绩不好，或者最不喜欢数学。许多人觉得，数学没有什么用处，无非是“聪明人的思想体操”，练练功夫而已。数学不能吃，不能穿，不能促进工农业生产，不会产生经济效益，不能……这些错误的见解都是从数学家的书斋里，数学教师的课堂上，数学考场的试卷内，曲折地流

淌出来的。概而言之,数学观的转变,是迎接明天的中国数学首先要解决的课题。

2. 数学的定义及其特征

《中国大百科全书》(数学卷)开宗明义写道:“数学是研究现实世界中数量关系和空间形式的。简单地说,是研究数和形的科学。”这是一个权威的论述,脱胎于马克思和恩格斯关于数学的概括。

对于这个定义,人们有各种不同的理解、补充和修改。例如,钱学森在《关于思维科学》一书中,把数学和哲学并列,认为数学是在社会科学和自然科学之上的一门学问。有人对数学来源于现实世界有不同的看法。比如,“哥德巴赫猜想”来源于现实世界的哪一个部分?很难说得清楚。记得 1958 年,武汉大学的齐民友先生写过“竹子的哲学”一文,内中认为数学的生长像竹子,根在大地,然后自己一节一节向上长,间或爆出新笋,长成新竹。若干年之后,竹子开花,结成种子,重回大地。这一比喻,何等贴切。但在当时,这是作为反对数学来源于实践的“反面教材”发表的。更多的数学家认为,现代数学的发展,已经超出“数”和“形”的范围,应当包括“结构”、“范畴”、“模型”等更广的对象。不过,只要把数和形作广义的理解,大概也就可以了。

关于数学的特点,一般沿用原苏联亚历山大洛夫的“三性”提法:抽象性、严谨性、广泛应用性。这一提法有合理的成分,但产生的实际效果却在很大程度上被异化了。一提数学,先就是抽象,使数学远离人们的实际经验和日常生活。其实,物理学和化学也抽象,“力”、“电压”、“当量”等等也不是看得见,摸得着的。数学的抽象在于它的对象:形式化的思想材料,而这些材料仍然可以溯源于经验世界,不必过于强调其抽象之难。至于严谨性,和逻辑联系在一起,使数学成为一门相对精确的科学。但是,过分地强调“严谨性”,把数学等同于逻辑,把生动活泼的数学思想淹没在形式演绎的海洋里,实在是歪曲了数学的本质。至于“广泛应用性”,乃是抽象性的推论,几乎没有新的论述。因为数学的“抽象”,使得数学虽然什么都挨不上,可又什么

都挨得上，于是到处都可以用数学，数学的广泛应用性也就成立了。这样的论述引申到中学数学教育上，便是绝口不提数学的应用。特级教师的论文中，绝少涉及应用。数学高考在相当长时间里不涉及应用题，学生视应用题为畏途，连老师也觉得头痛。到了这一步，数学除了“思维的体操”之外，再也没有什么可谈的了。数学教育变成解考题教育，数学教学的目的是通过考试，数学老师成了解题机器，解数学难题成了数学杂技，只要躲在“抽象性，严谨性”的口号下，什么“联系实际”、“数学为国家建设服务”、“培养用数学分析和解决实际问题能力”便统统不提了。

问题出在“数学观”已经跟不上时代要求。长期以来，数学的含义只包括“纯粹数学”。大百科全书中的数学定义，亚历山大洛夫的“三性”都是从纯粹数学的意义上来说的。其实，今天的数学，已经不再仅限于纯粹数学，而是已经渗透到社会生活的每个角落，成为能够立即转化为生产力的一门技术。每一种高科技的背后，都离不开数学的支持：电视卫星的姿态和定点控制必须用数学计算得分毫不差；数字电视主要依靠信息压缩的数学技术；头顶呼啸而过的喷气飞机的制造和飞行，是用数学方法加以计算和控制的；与人的健康紧密相关的 CD 扫描，其基本原理竟是一条数学定理——拉东逆变换公式；信息时代的国家机密正是通过数学密码理论才得以在传输过程中保证安全；庞大的世界经济的未来，正在由成千上万个未知数的微分方程组进行模拟和预测；出身北京大学数学系的王选院士用数学技术创立了享誉国际的“方正”集团。当我们在尽情享受数学文明的时候，我们应当如何认识当今的数学呢？

中国的数学观多半限于纯粹数学，有其历史原因。建国以前的旧中国工业凋敝，科学落后，没有应用数学可言。当时的著名数学家在艰难的条件下开展数学研究，没有经费，只能从很少花钱的纯粹数学着手，例如研究数论，函数论，微分几何。他们的成就是国家的骄傲，体现了中华民族的创造精神。但是也不可避免地带有时代的局限。建国以后，华罗庚、苏步青等都先后涉及应用数学，而且身体力行，力求有所作为。可惜的是，文化大革命时期的动乱搞浑了人的思

想。否定数学基础研究，批判纯粹数学研究工作，走向极端，把搞不搞应用数学当成“打人的棍子”，伤害了许多人。1976 年以后，拨乱反正，终于“进一步，退两步”，在一些地方，应用数学反倒成了“实用主义”的替罪羊。在中学数学圈子里，十年动乱期间搞“工业基础”、“农业基础”，数学课成了“划线”、“识图”，真的是实用主义的数学教育。

80 年代将它推倒重来理所当然。可惜的是，真正意义上的数学应用却渐渐从中学数学教学中消失了。进入了 90 年代，国家建设出现了繁荣期，科教兴国已成为基本的国策。在这样的时候，重新审视数学的价值，把应用数学提到战略地位来考虑，形成新的数学观，就是十分必要的了。当然，忽视数学应用的倾向也具有世界性，并非中国所特有，只是中国由于历史环境特殊，情形更为严重而已。

3. 三段“讲话”的共同主题：数学应用

以下让我们引用一些数学家的谈话来重新认识“什么是数学”。

(1) 钱学森讲话

1989 年 8 月 18 日，著名科学家钱学森在中国数学会的“数学教育与科研”座谈会上发言，提到了“数学技术”，全文发表于《中国数学会通讯》1989 年第 4 期。现将有关的段落摘引于此(为语气连贯，有一些文字上的改动)。

“在理科，工科的实际工作中，现在不是用手算，而是用电子计算机去算，去求解。去年，在四川的《大自然探索》杂志上，有美国布朗大学的谢定裕教授写的一篇文章，提出‘数学科技’的概念。文章说，50 年代热闹一阵的应用力学，现在都融化到各门工程课程中去了。所以应用力学大部分已撤消了。另一方面，应用数学的老师又都是数学家，对工程不感兴趣，所以应用数学又太纯数学化了。这样，数学的基础理论有了，工程技术的具体问题在这儿，中间怎么过去？不是靠手算了，是靠电子计算机。也就是说从自然科学的理论开始，用

电子计算机能得到具体工程技术问题的解答。那么谁来做这些中间的工作呢？在美国成立了一些新学术组织，如工业数学与应用数学协会(Society of Industrial and Applied Mathematics (SIAM))，国际工业数学和应用数学大会(International Congress of Industrial and Applied Mathematics (ICIAM))。他们都离开了老的领域，而利用计算机来工作，谢定裕教授把这称为'数学科技'，我想不叫'数学科技'，而叫'数学技术'。这要求数学给一个方法，能使科学的理论通过电子计算机解答具体的科学技术问题。这包括两个方面：第一是要会用计算机，会指挥它去算；第二是对电子计算机给出的解答，通过荧光屏的显示，能够理解它，别让它给唬住了。我觉得后一个关于理解问题，要求从宏观的、正确角度去认识，这也是数学问题。这里我可以举几个例子。比如我从前做过的工作，理想气体流过一个给定的物体，这在航空技术里是一个根本的问题。当时，出现这么一个怪事：当理想气体，即可压缩的非黏性气体，流过一个等速运动物体时，运动的速度跟远处理想气体声速之比，如果超过一定的数值，但比一小，好象这个解是不存在的。当时我们把这个连续解不存在的马赫数，叫高临界马赫数。30 年前，我们搞具体工作的人猜测大概有这样的搞浑了高临界马赫数，这实际上是一个解的存在问题。再一个问题，真实的有黏性的气体，当流体的雷诺数达到一定数值时，就会出现湍流，现在叫"混沌"。过去对这个研究费了很大的劲，也没真正解答。现在从新的混沌概念出发，要问为什么有时候有混沌发生，什么时候会出现？这也是解的宏观性质问题。

从以上例子来看，我觉得自已以前学的那套数学，不能应付现在的实际。上百年的这套老东西脱离实际太远了。今天的实际要求学生学会两条：一要会用电子计算机，二要能理解计算机给出的答案。"

(2) 国际数学家联盟主席 D·芒福特(Mumford)答记者问

1995 年 5 月，国际数学家联盟(IMU)在巴黎举行执委会。有记者问道"您个人认为 21 世纪数学将面临怎样的挑战?"芒福特的回答是：

“啊！这可真是一个重大问题，人们需要坐下来，长时间地思考这个问题。我个人感觉到，一个十分重要的问题是恢复纯粹数学家和应用数学家之间的思想交流。在 19 世纪，您可以看到大多数数学家都是身兼二任，例如傅立叶级数，就是受了应用的刺激。但以后产生了分隔，尤其是在美国。我想其他国家在某种程度上也是如此。我希望当前对科学用处的普遍强调（这有利于公众对科学的投资），将不至于简单地花很多钱去搞纯粹数学研究，而是相反，应当引向一个共同目标，使得纯粹数学研究人员能在应用中受到启发，运用他们的理论思想更有效地解决实际应用问题。”

请注意：D·芒福特本人是一位纯粹数学家。1937 年出生，美国哈佛大学教授。研究方向是代数曲面，以研究代数族的结构和存在性而著名，1974 年获得世界数学最高奖——菲尔兹奖。一位纯粹数学的名家发表上述谈话，更是意味深长。

(3) 姜伯驹院士在数学与力学教学指导委员会的讲话

姜伯驹院士是北京大学教授，专长拓扑学，在不动点类理论上有突出贡献，获第三世界科学院颁发的数学奖。他是国家数学与力学教学指导委员会主任。1996 年 5 月，他在该会第二次工作会议上发表讲话，作为一个纯粹数学家，他同样呼吁重视数学的应用：

过去讲数学的重要性，就是两句话：数学是思想的体操，数学是科学的语言。现在，数学已经不必通过其他的学科，而直接在科技前沿发挥作用了。很多高精尖的东西取决于数学模型的控制。数学已经走到前列了。

许多事情，特别是有竞争的地方，数学往往是最后取胜的法宝。数学用得好，你就赢了。

数学在 20 世纪下半叶有很大的发展，其中最大的发展是应用。

数学已从幕后走到台前，直接对生产过程、经济管理、科技发展产生作用。以前只关心代数、几何、分析的数学家，现在必须面对工程控制、图像处理、模糊识别、运筹优化等一系列的应用数学学科。

4. 从事数学研究的魅力

在美国,当一个数学家,年薪不过几万美元,过十万美元的已是凤毛麟角。1996 年,一个英国大学毕业的数学博士到不同行业工作的年薪差异如下(单位:万美元,都以 12 个月计算):

	最　低	中位数	最　高
数学教学或研究	1.50	3.30	7.20
政府机关工作	3.60	4.27	6.50
工　商　企　业	2.50	5.80	10.00

显然,刚毕业的数学博士如到工商企业,华尔街金融市场工作,薪金将会明显高于在大学或研究所从事数学教学或研究。这种情形,当然会导致数学人才流向数学圈子之外。但是这也不必过于担心。首先,数学人才到其他部门去工作是一件好事,实际上有利于数学市场的开拓,扩大数学在公众中的影响力。其次,数学的教学和研究工作的魅力,会把那些最优秀的数学青年吸引进来。探索数学的奥秘,一直是许多人的梦想。稍少的薪水,挡不住当一名数学家的诱惑。

那么,数学研究有什么吸引人的地方?

数学研究的第一个特点是数学的精确性。数学是一门精确科学,结论是对是错壁垒分明,没有什么争论。虽然它的价值有时也不能立刻显示出来,但是至少不会今天说它对,明天说它错,就象某些学科那样,随政治和社会的变迁而大起大落,数学的评价标准,是比较稳定的,客观公平的,而且具有很强的国际一致性。这使得数学研究成果,很快就能判断其真假,而且能够经受时间的考验,得到国际同行的承认。

有一个故事说:原苏联的大数学家柯尔莫哥洛夫本来想研究历史学,并写了一篇论文。一位历史学家看了他的论文后说,你文章中的结论,只得到一个论据的支持,那是不够的。这就是我们常说的

“孤证不足为凭”。柯尔莫哥洛夫对此很不以为然。他说他想研究一门学问,其中的一切结论只要一个证据就够了。于是柯尔莫哥洛夫转向了数学,此后历史学界失去了一位天才,而数学界则是幸运的。

20 世纪 80 年代末,中国著名大学的校长几乎都是数学家。丁石孙(北京大学),王梓坤(北京师范大学),谷超豪(中国科技大学),伍卓群(吉林大学),齐民友(武汉大学),李荣华(中山大学)。分析这种状况,很多人认为是数学家具有较强的逻辑思维能力,因而善于做行政工作。其实,数学家当校长的主要原因在于数学的特点,即他们的数学成就不因十年动乱的政局变化而受损伤。他们的数学成果容易得到国际同行赞赏。经过十年动乱,与其他专业比较而言,数学家的学术地位相对地容易确立,容易获得大家的承认。推举有学术地位的人做校长,是自然的事了。至于说数学家的逻辑思维能力强,因而行政能力也比较强,恐怕就难说了。许多行政领导遇到的问题,大多是没有逻辑解的,如果硬要用逻辑方法去处理,其效果恐怕会适得其反。事实上,到了 90 年代,上述学校的校长恰恰都不再是数学家了。

数学研究的第二个特点是突现个人智力的角逐。数学较少涉及对经费、设备的依赖,可以充分自由地发挥个人的特长。十年动乱时期,社会科学因为政治原因已经不可能进行研究。自然科学的情况稍好一些,但大多数的学科受到设备、经费的限制,无法真正启动。唯独数学,无需多少经费,弄几本书或论文就可以研究起来。陈景润在那样艰苦条件下可以研究数学,却不可能到实验室做物理化学实验。1990 年前后,数学界的工作屡屡见诸报端,原因也是在文革时期还能偷偷地做一些纯粹数学的工作。1978 年,恢复高考和研究生考试之初,许多优秀数学人才就像从地下冒出来一样,一些“小木匠”、“县剧团编剧”、“农场工人”,连升三级成了数学博士。原来他们都是自己偷偷学出来的。

此外,数学研究的竞赛规则是“胜者为王”,只有第一,没有第二。一个数学结果如果别人已经做出来,并为人所知了,那么你的重复就没有发表价值。这里不存在“填补国内空白”的说法。正因为如此,

数学工作都必须是创新的，前人所没有的，完全是一种公平的智力角逐。为了国家的荣誉，民族的尊严，许多有志之士，愿意在数学战场上为国争光，将是可期的。数学的魅力，引得无数英雄竞逐。像陈景润那样，茶饭不思，为伊消得人憔悴的数学家，一定会代有人出的。

数学研究领域中主要是个体劳动，合作的情况也有，但也是少数人，不可能集体创作。在数学研究过程中，可以自由地按照个人的思路去进行。数学论文的正确与错误，相对来说比较容易判断，权威的压制也要少些。这一特点吸引无数的青年人投入数学竞争，并为之奋斗终生。

以上的两个特点，在现时仍然保持着。数学之深奥，数学之神奇，数学之美丽，数学之自由创造，还会不断吸引大批青年投身数学研究事业。但是，说研究数学“不要花钱”的说法，也许需要修正。目前，计算数学、应用数学都需要投入大量的实验设备，高性能的电子计算机，以及价格不菲的数学软件。即使是做纯粹数学研究，也要用计算机试算许多例子，从中观察规律，做出猜想，然后再进行证明。总之，时代在变，一些老的观点也会随之变化，不过，数学的魅力将会是永恒的。

第三节　核心数学的未来

纯粹数学主要包括代数与数论、几何与拓扑、分析学三大部分，核心数学指纯粹数学的核心。数学是一个整体，一些最有价值的数学问题、具有重大发展潜力的数学理论和方法构成一个时期的“核心数学”。它由时代的社会需要所决定，也随当时领袖数学家们的活动而形成。正如流行的时装那样，既有服装设计师的提倡，更是人们对时尚的一种心态反映。发展一个国家的数学，必须从核心数学入手，这样才会有扎实的根基，具备创新的能力。

1. 核心数学的形成与特点

核心数学的内容并非是固定不变的。它的发展常常受到其他科学分支以及应用数学内容的影响和推动。但是，核心数学发展的主要推动力来自数学的内部。从 19 世纪的数学来看，复数理论因负数开方引起；伽罗瓦的群论来源于方程的根式解；罗巴切夫斯基的非欧几何学起始于对欧氏几何的第五公设的研究；而数学分析的严密化进程，则导源于无限小量之比的不确定性。这些数学内部提出的问题，深刻地反映了客观世界的数量关系，揭示了丰富的数学内涵。当然，许多应用性的问题，也会成为核心数学的重大分支。最好的例子是傅立叶从热传导提出的三角级数展开。傅立叶分析、傅立叶变换、傅立叶算子、群上调和分析、非交换调和分析，其影响至今不衰，始终是核心数学的重要组成部分。

在 20 世纪的上半叶，爱因斯坦的相对论和量子力学诞生，与之相应的黎曼几何、李群和泛函分析当然属于那时的“核心数学”范围；

传统的函数论、数论等基本的数学工具，当然仍是核心数学的一部分；此时，组合拓扑学，以一般理想论为代表的抽象代数等，虽然并不和需要相联系，却以旺盛的生命力迅速发展，也构成核心数学的中坚。另一方面，盛极一时的射影几何学、特殊函数论、方程式论、四元数解析等学科则渐渐淡出。

到了 20 世纪下半叶，电子计算机的出现导致数理逻辑、逼近论等学科的发展；与此同时，微分几何学受到拓扑学的影响产生了整体微分几何，又和规范场论等数学物理课题相结合，从非主流数学进入主流数学；微分方程求解历来是核心数学的重要部分；流形上的分析、多元复分析、动力系统、指标定理等成为世人关注的数学课题；完全受数学内部需要而发展的代数数论、代数几何，更以费马大定理的证明而达到高潮。但是，一些意义不大的探究细枝末节的研究课题则从主流地位消退，例如一般拓扑学、函数论和泛函分析中的某些分支。

面向 21 世纪的中国数学，应当如何看待当前和未来的核心数学呢？中国自然科学基金会的一份研究报告认为，核心数学的重要科学主题和研究方向是：

- 解析数论、代数数论与代数几何(包括构造性代数几何)。
- 群与代数及其表示理论。
- 流形与复形拓扑学。
- 整体微分几何。
- 经典分析的前沿问题。
- 随机分析和无穷维分析。

这六个课题中，除了解析数论和经典分析之外，都是我国过去的薄弱环节。80 年代以来，一批年青数学家开始追赶，有所突破，但是就总体上而言，仍和世界先进水平有很大的差距。在今后的一段时间内，它们仍是我们的努力目标。

核心数学的重大进展和其成果的实际应用都是难以预计的。核心数学课题一旦有所突破，常常会产生不可估量的影响。伽罗瓦提出的群论，源于代数，后来扩展到几何变换群、拓扑学中的同伦群和

同调群、微分方程中的李群、有限群和典型群、物理学中的对称群、规范群，其覆盖面几乎是整个数学。至于群论直接用于密码编制，成为一种特殊的数学技术，更是始料所不及了。

陈景润研究的“哥德巴赫猜想”，迄今仍领先于世界的“1＋2”，它能否用于其他数学学科的研究？会不会有实用价值？目前都还说不上。但是，这不妨碍陈景润是中国最好的数学家之一，也没有人怀疑这一成果的重要性。至于它的实用价值，相信也会在某一天获得体现，只是现在无法预料就是了。

但是，并非任何纯粹数学问题都能算做核心数学。只有“好”的纯粹数学，即正在生长、意义重大、影响全局的数学才能进入核心数学的范围。

2. 陈省身寄语：做“好”的数学

要想把中国建设成为世界数学大国，国际数学大师陈省身一再希望中国的数学家，尤其是青年数学家：“一定要做好的数学”。难道数学还有“好”、“坏”之分吗？许多人会觉得是件新鲜事。

按国内过去的一般看法，数学研究工作要么对，要么错，很难说好坏。只要逻辑上正确的数学论文便可发表。能发表论文，能把别人论文里的结果加以改进，做些推广，便是数学家，如果能得到外国人的称赞，便是著名的数学家了。这种看法，用较低的标准来衡量，也有道理。科学研究就是发人之所未发，只要别人没有做过的数学问题，你做出来了，总是有成绩的，应该鼓励。但是，若从高标准来要求，要到世界上去竞争，要建成数学大国，那么就要看你做出来的数学问题的意义如何了。这里有“优劣”、“粗细”、“好坏”、“新旧”之分。当今世界上每年发表的论文，多数是比较平庸的，意义不大的，在已有工作上做一些枝节的推广和改进，没有多大的创造性，真正重要的文章实在不多。相比之下，我国数学工作者的人数，发表论文的数量，绝对数量不算太少（至少比欧洲的一些小国家要多），但论质量，则达到上乘的是极少数。

陈省身 1985 年在南开数学研究所成立时就提出:"让青年人知道有"好的数学"(指有意义,有创新)和"不好的数学"(指仅限于把他人工作推演一番)之分,从年轻时就懂得欣赏"好的数学"。

1992 年,陈省身在庆祝中国自然科学基金会成立十周年的学术讨论会上再次详细论述这一问题。他说:

一个数学家应当了解什么是好的数学,什么是不好的或不太好的数学。有些数学是有开创性的,有发展前途的,这就是好的数学。还有一些数学也蛮有意思,但渐渐地变成一种游戏了。

下面举例来谈谈。大家也许知道有个拿破仑定理。据说这个定理和拿破仑有点关系,它是说,任何一个三角形,在其各边上各作等边三角形,然后将这三个三角形的重心联结起来,一定是一个等边三角形。各边上的等边三角形即可以朝外面作也可朝里面作,于是可得到两个解。这个数学就不是好的数学,因为它难以有进一步的发展。当然,你做事累了,坐在沙发上愿意想想这个问题,也蛮有意思,这好像一种游戏,可以解闷。

那么什么是好的数学呢?比如解方程就是。搞数学都要解方程,一次方程容易解,二次方程就不同,$x^2-1=0$ 有实数解;而 $x^2+1=0$ 就没有实数解。后来就加进复数,讨论方程的复数解。大家知道的代数基本定理就是 n 次代数方程必有 n 个复数解。这一问题有很长的历史。当年有名的数学家欧拉(Eular, 1707—1783)就考虑过这个问题,但一直没有证出来。后来还是高斯(1771—1855)证出来的。还发现复数和拓扑有关系,有了新的理解。因为复数减 1 的绝对值等于 1 就表示一个圆周,在这一圆周上就有很多花样。

如果从解 $f(x)=0$ 到解 $f(x, y)=0$, 那就进入到研究曲线,当然也可能没有解,一个实点也没有。于是花样就来了,假使你在 $f(x, y)=0$ 中把 x, y 都看成复数,则两个复数相当于四维空间。这就很麻烦,出现了复变函数论中的黎曼曲面。你要用黎曼曲面来表示这个函数,求解原来的方程 $f(x, y)=0$, 那就要用很多的数学知识,其中最要紧的概念是亏格。你把 $f(x, y)=0$ 的解看成曲面之后,那么曲面有多少个圈、球面、环面等等的不同花样都和亏格

有关。

此外，你也可以有另外的花样，比如 $f(x, y) = 0$ 的系数都假定为整数，你也可以讨论它的整数解，这就很难了。

这段论述明确地指出了什么是好的数学，即那些有深远意义，可以不断深入影响许多学科的数学课题。像方程这样的数学思想，其价值是永恒的，不断发展的。所以说它是好的数学。

1995 年 11 月，陈省身在上海数学会的报告，再次论述了这一问题。他引用 18 世纪的法国大数学家拉格朗日(Lagrange，1736—1813)的标准，认为好的数学问题应满足两个条件：1)易懂。走在马路上向任何一个人都能讲清楚；2)难攻。这种数学问题必须相当困难，但又不是无法攻克的。符合这两个条件的数学问题不是很多。德国大数学家希尔伯特在 1900 年提了 23 个数学问题，都是好的问题，对本世纪的数学发展起了很大的作用。陈省身在上海的报告中也指出，像费马(P. de Fermat 1601—1665)大定理：

求不定方程

$$x^n + y^n = z^n (n \geqslant 3)$$

的正整数解。

一看就明白题目的意思。再如三体问题，即研究太阳、地球、月亮三个星体运动的轨道方程，也是不难懂的。这两个题目都很难，却都能着手工作。费马大定理终于在 1995 年被 A · 怀尔斯(A. Wiles)彻底地证明了。三体问题也陆续有所进展。

陈省身在上海的报告中，还顺便提到了中学生数学奥林匹克竞赛题。他说，我是支持数学竞赛的，对数学竞赛的获奖者也一再给以鼓励，希望他们成功。但是数学竞赛题目都不是好的题目。因为在两三个钟头里由青少年学生能做出来的技巧性题目，不可能有很深的含义。这样说，并不是说奥林匹克竞赛题目都出得不好，其含义是，数学奥林匹克竞赛得奖只是一种能力的表现，离开研究一个好的数学问题还差得很远，更不可把奥林匹克数学竞赛获奖者等同于数学家。

那么，好的数学和当前国际上的主流数学有什么关系？陈省身曾解释说："所谓主流数学，是指一个伟大的数学贡献或深刻的定理，其涵义很广，证明也很不简单。如果要在当前选一个这样的贡献，我想那就是阿蒂亚-辛格指标定理。这个定理可说是 $f(x, y) = 0$ 问题的近代发展，即将代数方程、黎曼曲面、亏格理论等等从低维推广到高维和无穷维"。主流数学当然是重要的，研究和学习它是非常要紧的。但是陈省身认为，数学的方向很多，又是个人的学问，不一定大家都去做主流数学，"我倒觉得可以鼓励人们不在主流数学上做。最理想的情形是，现在做的不是主流，而过几年却成为主流了"。陈省身也常常用他自己的经验来说明这一点。第二次世界大战之前，微分几何不是主流，甚至被认为"它已经死了"。但到了本世纪的下半叶，微分几何却成了主流。陈省身也因先行一步，而成为大范围微分几何的奠基人。陈省身还指出世界上有一些小的国家，他们着重在一些自己擅长的领域内工作，如本世纪初的波兰，着重集合论、泛函分析；芬兰则主攻复变函数的值分布，在这一领域拥有世界上最好的专家。这样，有自己的特点和专长，同样会对世界数学做出重大贡献。

做好的数学，当然需要能力。就像在茫茫沙漠里找石油，这需要能力去识别，胡乱打井怎么行？数学也是一样，有能力做好的数学的人都是用功的，当然用功也有不同的形式，例如德国莱比锡的范·德·瓦尔登(van der Weardon，公元 1903—1992)，是一天到晚坐在书桌前做研究，而康福森(S. Cohnvossen 公元 1902—1936)却是成天走来走去想数学，像是在游荡。但两人都是有成就的数学家。

3. 核心数学的一座高峰：费马最后定理

常言说，问题是数学的心脏。重大的数学问题可以吸引几代数学家，甚至几百年的努力。最好的例子就是前面说过的费马大定理：

$$x^n + y^n = z^n (n > 2)$$

没有正整数解。(当 $n = 2$ 时,这就是勾股定理。它显然有整数解。)

费马,法国数学家。1637 年前后,他在阅读 3 世纪希腊数学家丢番图(Diophantus)的《算术》一书时,在某一页的边上写了这样的一段话:“不可能将一个立方数分拆成两个立方数,一个四方数分拆成两个四方数。一般地说,任何次数大于 2 的高次方数都不能分拆成两个幂次相同的高次方数。我已找到这一定理的绝妙证明,可惜这里空白太小,写不下”。

费马是一位大数学家。他在微积分的发明、不定方程、数论研究上有许多传至后世的工作。费马在数论方面的猜想和有关问题,都由后人一一加以解决,唯独这一“空白写不下的绝妙证明”却一直没能完成,所以数学史家称之为“费马最后定理”。

$n = 4$ 的情形,费马本人给出了证明。约 100 年之后,欧拉在 1753 年解决了 $n = 3$ 的情形。$n = 5$, $n = 7$ 时的证明也在 1825 年和 1837 年先后得到。19 世纪 50 年代,库默尔(Kummer, 1810—1893)用分圆域方法将结果大幅度推向前进。到了 20 世纪的 70 年代,已经证明了费马定理对 $n < 125\,000$ 的整数都是对的。但是离开完全解决费马定理还差得很远。经过 300 年无数大数学家的努力,这一难题未能最后解决。看来,费马当时所给出的“绝妙证明”是靠不住的。

正面突击费马最后定理久攻不下,数学家遂另辟蹊径,将 z^n 除过去,令 $u = \frac{x}{z}$, $v = \frac{y}{z}$,则费马大定理可以改写成:$u^n + v^n = 1$ 没有有理数解。

从几何观点看,这是一条 n 次曲线。问题化为怎样的平面曲线不含坐标为有理数的点。于是有理数域、有理数域的扩张、椭圆曲线、椭圆模曲线等等代数数论方面的问题就和费马定理证明联系起来了。50 年代,日本的志村五郎和谷山丰猜测“每一条椭圆曲线都是椭圆模曲线”。如果猜想成立,费马定理将是它的一个推

论。1993 年 6 月 13 日，在美国普林斯顿高等研究院工作的英国数学家怀尔斯在英国剑桥大学牛顿研究所的一次会议上宣布："半稳定的椭圆曲线都是椭圆模曲线"，再引用里贝(K. Ribet)在 1986 年的一项结果，即可证明费马最后定理。消息传出，轰动全球。位于美国旧金山伯克利的"国家数学研究所(MSRI)"在大剧院举行报告会，15 美元一张的门票，被炒到 25 美元。

不久，怀尔斯发现证明有一个漏洞。一年之后，他和他的学生 R·泰勒(Tayler)将原证明作了修正，国际数学界认可了这一结果，350 年的悬案终于尘埃落定。费马定理是正确的。

这是一场典型的人类智力竞赛，胜者为王。怀尔斯是 20 世纪最后十年内的数学英雄，永远载入数学史册。数学界的最高奖——菲尔兹奖有一项规定，获奖者必须在 40 岁以下，怀尔斯刚刚超过，因而无缘获此殊荣，但是他获得了另一份数学最高奖——沃尔夫奖。

华罗庚的学生陆洪思在《科学》杂志(1996 年)上撰文介绍费马定理的证明过程，并且谈到华罗庚在 50 年代的一些设想。文中提到，华罗庚曾打算开展现代代数几何和局部紧群表示论的研究，介绍过当时很新鲜的"有限域上代数曲线黎曼猜想的证明和应用"。1956 年的科学发展纲要中列入了"发展模形式"的设想。可惜的是，50 年代后期的政治运动中断了这一计划。60 年代初，华罗庚又准备带领研究生对自守形式和表示理论开展研究，文革动乱再次使计划夭折。如果这些计划能够得到实施，中国数学家也许可以在费马定理的研究中占有一席之地。但是，历史是不能重写的，这些只好作为历史教训加以汲取了。

人类花这么大的力气证明费马定理有何价值？首先，数学文化是人类文化的组成部分，正如攀登珠穆朗玛峰构成人类文化的一部分那样，它显示出人类的智慧和能力，成为一种伟大的科学象征；其次，在研究过程中涉及许多深层的数学成就，将是一系列数学分支的出发点；最后，研究过程中的副产品——二元域理论，则是当今信息传播中不可或缺的数学基础。

4. 21世纪的数学问题

国际数学联盟(International Mathematical Union 简称 IMU)负责召开每四年一度的数学家大会。在1900年的国际数学家大会上,希尔伯特所提出的23个数学问题,给20世纪的数学打上了深刻的烙印。现在,21世纪已经到来,我们为新的世纪提出怎样的数学问题呢?受IMU的委托,蜚声世界的俄罗斯数学家阿诺尔德(Arnoldl 1937—)向一些数学家发信,请他们描述21世纪将会研究的重大数学问题。确实,现今的数学面广量大,分支既多又细,已不是一个人可以驾驭的了。因此,IMU希望由阿诺尔德牵头,集中当今主要数学家的智慧,来预测未来数学的发展。这些预测将会陆续发表。

1997年6月,在加拿大多伦多的"菲尔兹数学研究所(Fields Institut for Mathematics)"举行庆祝阿诺尔德60寿辰的学术讨论会。S·斯梅尔(Smale)在会上作了"未来世纪数学问题"的报告,作为对阿诺尔德信件的答复,这份讲稿在1988年广为流传。

斯梅尔,1932年出生于美国密西根州,密西根大学数学博士(1956),先后在芝加哥大学、哥伦比亚大学、加州大学任教授。早期从事微分拓扑学研究,1966年因证明广义庞加莱猜想而获菲尔兹奖。此后以建立现代抽象的动力系统而闻名。斯梅尔的研究领域很广,包括运筹学、数理经济学、统计力学、湍流等。后来又有计算复杂性的著名工作问世。1995年来到香港九龙的城市大学任数学教授。斯梅尔的讲稿在《Mathematics Intelligencer》1998年第二期上发表。其中提出了18个未来世纪的重大数学问题,这里摘引18个问题的标题(有些有较完整的陈述)。

● 黎曼猜想。

黎曼函数 $\zeta(s) = 1 Re(s) > 1$ 的所有位于 $0 < Re(s) < 1$ 中的零点都集中在直线 $Re(s) = \frac{1}{2}$ 之上。

- 庞加莱猜想。

若一个紧3维流形M上的每一个圆周都能形变收缩为一点，则M和3维球面同胚（$n > 4$ 的情形由斯梅尔于1960年解决，福利德曼在1984年证明了 $n = 4$ 的情况。现在只剩下 $n = 3$ 的情形了）。

- $P = NP$？

令 Z 表示由0，1两个元素组成的域。设输入了 k 个系数在 Z 中的 n 元多项式，试问能否有一个多项式时间算法来判定它们有没有公共零点？（多项式算法是指这样的算法：它的计算步数由各多项式系数数目的一个多项式所界定。）

- 多项式的整数零点。

一个整系数的多项式 $f(x)$，其整数零点的个数能否被某不变量的多项式所界定？

- 丢番图曲线高度的界。

要判定一个整系数多项式构成的丢番图方程段 $f(x, y) = 0$，能否在 S^C 之内判定它是否有整数解？S 是多项式的“高度”，C 是某常数。

- 天体力学中相对平衡态数目的有限性。

若 n 个天体的质量为 $m_1, m_2, \cdots, m_n$，问这些天体的相对平衡态的数目是否有限？

- 2维球面上点的分布。
- 把动力学引进经济学理论之中。

把一般的经济学均衡理论的数学推广到包含价格调节的情形。

- 线性规划的多项式时间计算问题。
- 流形上可微逼近的封闭定理。
- 一维动力学通常是双曲的吗？

一个复多项式 T 能否被某同次的多项式 P 所逼近，P 的每个临界点经过叠代会趋向一个周期汇(Periodic Sink)？

- 微分同胚的“中心化子”。
- 希尔伯特的第16问题。
- 洛仑兹吸引子。

洛仑兹方程的动力学系统是否就是几何洛仑兹吸引子的动力系统？

● 纳维-斯多克斯(Navier-Stokes)方程。

这一流体力学基本方程在3维域中有唯一的整体光滑解吗？

● 雅可比猜想。

多项式映射的每点都是非奇异的，是否必定一一对应？

● 解多项式方程组。

以多项式时间找到一个零点的统一算法。

● 人工智能是否有极限？

指人工的和人类的智能是否有极限？极限是什么？

斯梅尔在选择这18个问题时的原则是：

第一，陈述简单。当然这只是相对而言，对非专业数学家来说，这些陈述并不简单，但在现代数学的文献中，这已是相当简明的问题了。

第二，斯梅尔本人比较熟悉，但已发现这些问题不容易解决。

第三，问题十分重要。即使是部分结果，或者是解决问题的任何努力都会对数学发展产生重大影响。

斯梅尔特别提到前三个问题是特别重要的。

第四节　应用数学和数学技术

一些哲学家总喜欢谈论三次数学危机(分别由无理数发现、无穷小运算和罗素悖论所引起)。事实上,数学在一日千里地发展,现在正是蓬勃生长的数学黄金时代。计算机技术的出现,使数学获得前所未有的原动力。除了说纯粹数学的无序膨胀会导致某种程度的调整之外,社会对应用数学的需要与日俱增,特别是为解决实际问题而诞生的种种数学技术,已从过去的"幕后数学编剧",成为当今的"台前数学主角"。未来的数学必将沿着这条康庄大道继续前行。

1. 新闻和故事:数学技术的巨大作用

对大多数人来说数学技术还是一个陌生的名词。让我们来看看有关数学技术的一些新闻和故事。

(1) 抗洪斗争

1998年9月7日,上海《文汇报》报导:"20吨炸药进入倒计时,最后一刻共和国决策者决定荆江不分洪。"其中有一段是这样写的:"由多方专家组成的水利专家组用'有限单元法'对荆江大堤的体积渗漏进行了测算,确定出一个安全系数。照这一系数推定,沙市水位即使涨到45.30米,也可以坚持对长江大堤严防死守、不用分洪。"这里提到的"有限单元法",就是求解微分方程边值问题的一种数学方法。我国已故数学家冯康(1920—1996)是这一方法的首创者之一。他在1966年文化大革命开始之际发表论文,国内外知道的人比较少。在此同时,西方数学家做出了类似的成果。1982年国际数学家大会在华沙召开,冯康应邀作5分钟报告,这标志国际数学界对冯康

首创有限单元法的承认。此会后来因波兰政治局势缘故延至 1983 年,冯康也因我国代表权问题未获解决而未去出席。有限单元法的用途十分广泛,在 1998 年抗洪斗争中用于大堤的强度计算,当是数学技术巨大作用的体现。

(2) 数字化电视

1998 年 5 月,上海的《科学》杂志发表中国科学院前院长周光召的文章“若干基础科学的发展趋势”。其中有一段提到数学,“作为一门基础学科,数学对当今生产也有巨大作用。例如,在信息传输过程中如何压缩信息是一个重要问题,而数学在这方面就大有可为。现代数学中有一门学问叫做小波分析,它在信息压缩技术中有重大作用。日本在发展高清晰度电视的竞争中落后于美国,就是因为信息压缩技术不够先进。美国应用数学研究成果发展信息压缩技术,在高清晰度电视及网络传输方面领先于日本,成为世界上信息技术最先进的国家”。

众所周知,日本在常规电视生产上占有优势,可是在数字化的高清晰度电视上却败下阵来。1993 年,美国有四家集团从事高清晰度电视的方案测试,GI 公司,麻省理工学院最先取得突破,以后四家的指标互有长短,但是同时参加竞争的日本“模拟 MNESE”方案明显不如美国方案,不得不退出竞争。此后,四家集团合作构成“大联盟”方案,成为数字化电视的制式标准,今后各国必将仿效,这就抢得了未来的商机。正如周光召的文章所说,诞生于美国的小波技术——一种信息压缩的数学技术,在其中起了关键的作用。

(3) 通讯网络

这是一个真实的故事。80 年代的某一天,美国著名的贝尔电话公司遇到了一件怪事:要求在一片荒无人烟的沼泽地上安装一部电话。事情是北卡罗林那大学提出来的。这所大学有三个分校,位于一个等边三角形的三个顶点上。按照贝尔电话公司的收费标准,如要在三校之间安装直接可以联络的电话网,需要按三角形的两个较短边长度之和收费。现在大学向贝尔公司提出,要在等边三角形的中心装一部电话,然后将中心和三顶点相连,依照规定,现在的电话

费以中心到三顶点连线长度之和收费。假定正三角形的边长是1，那么原来要按长度2交费，而在中心(沼泽地)上安装电话之后，只需按$\sqrt{3}$交费了。

贝尔电话公司的研究部主任意识到，北卡罗林那大学的能人在向公司挑战。沼泽地上按电话需要花费人力物力，到头来却少收电话费，岂不是赔了夫人又折兵？于是赶紧向北卡罗林那大学打招呼：沼泽地的电话不装了，电话费照原来的八五折收费，即和$\sqrt{3}$差不多。同时，主任连忙提出一个研究课题：看看贝尔电话公司的收费标准中是否还有别的空子可钻？打八五折收费是否已到了极限？这一研究任务落在一个中国访问学者——来自中国科学院应用数学研究所的堵丁柱的身上。经过一段时间的努力，堵丁柱终于证明：按通讯网络中的现行收费标准，不论如何安装新电话，减少收费的比例不会低于$\frac{\sqrt{3}}{2}$(近似于八五折)。堵丁柱的数学工作直接成为公司进行决策的一种数学技术。

通讯网络中的数学问题还有许多未获解决。一个通讯网络在数学上是一个图，其中顶点是电话，电话线是图中顶点间的连线，要使得任何两部电话之间可以通话，当然无须将任何两点间都直接连上线，那太浪费了。我们可以通过其他一些点中转，一个图的各点间需要中转的最低次数称为图的直径，通讯网络的直径愈小愈好。另外，我们还要求网络图中封闭的"圈"越大越好。一些顶点构成的集合，它们能直接联上的顶点数越多越好(图的放大倍数越大越好)。要求这么多，怎样设计才好？图论专家发现，图的联络矩阵的次根很有用处。

设图G有n个顶点，$a=1$或0表示顶点之间直接相连或不相连，这样可以得到一个$n\times n$的方阵，即图的联络矩阵。它的特征根都是实数，依次排下来，绝对值第二大的根称为次根。假设我们的电话网络允许每一部电话至多能和k部电话直接相连，此时的图称为k连通图，我们把次根不超过$2\sqrt{k-1}$的图称作拉马努杨图。现在的

问题是，如果 k 是定数，那么是否有顶点数可以无限增加的拉马努杨图？这对新装电话的配置很重要。解决拉马努杨图问题需要用到很深入的代数数论知识，特别是用到拉马努杨猜想。拉马努杨(S. Ramanujan 1887—1920)是传奇的印度数学家，他没有受过正规的大学教育，通过自学，用自己的数学直觉，在笔记本上写下了许多公式和结论。它们多半没有证明，但绝大多数都是正确的。他是如何思考的，至今仍是谜。他有一猜想：考虑无穷乘积

$$\varphi(s)=\prod_{p}(1-\lambda_{p}p^{-s}+p^{k-1-2s})^{-1}$$

的二次多项式 $1-\lambda_{p}s+p^{11}s^{2}$ 具有虚根

$$|\lambda_{p}|<2p^{\frac{11}{2}}。$$

这一猜想在 1974 年由比利时数学家德林(P. Deligne, 1940—)所证明，并因此而获得菲尔兹奖(1978)。利用这一拉马努杨猜想，1988 年，数论学家构造出了拉马努杨图，这又是现代数学史上的一段佳话。

2. 方正集团的启示

王选，中国科学院院士，中国工程院院士，北京大学教授，激光照排实现汉字印刷术革命的创造者。如果说陈景润是 80 年代中国知识分子的代表，其特征是个人忘我地进行科学研究，那么王选就是新时期的知识分子代表，其特征是把科学转化为生产力，使科学和企业联姻。碰巧的是，这两位都是数学家。

让我们来叙述王选教授的业绩。

他 1937 年出生，江苏无锡人。曾就读于上海南洋模范中学，1958 年毕业于北京大学数学系，从事计算机科学的研究。

1975 年，国家有一个“758 工程”，即汉字信息处理系统工程，其中有三个子项目：汉字通讯，汉字情报检索，汉字精密照排。当时国际上的电子分色机技术状况是：光学机械式的二代照排机前途不大，

字模管式三代机和飞点扫描式三代机正在走下坡路，数字存储的第四代技术将占主要地位。当时全国有五个单位在从事这项研究，但是有两家选择了二代照排机方案，另外三家选择了飞点扫描、字模管、全息模拟存储的技术途径。王选毅然选择了“数字存储”的方案，跳过二、三代，直接研制第四代技术。这样做，困难虽大，却符合了数字化的信息技术的发展方向。

汉字字形信息量太大，数字化的困难是西方文字照排无法相比的。王选说“由于我是数学系毕业，所以很容易想到信息压缩，即用轮廓描述和参数描述相结合的方法描述字形，并于 1976 年设计出一套把汉字轮廓快速复原成点阵的算法[1]，但那时的计算机速度很慢，复原点阵需要的时间很长”。如果王选只有数学和软件的知识，他也就打退堂鼓了。然而他有微程序和软硬件的知识，就采用专门硬件配合微程序，使速度提高了几十倍，初步克服了困难。1976 年夏，他终于决定跳过二、三代机，直接研制“激光照排系统”。

到了 80 年代，轮廓描述西方文字的做法在国外大为流行，当时已由轮廓发展为三次曲线轮廓。由于王选的研究起步早，很快吸收了国外的一些经验，发明了高分辨率字形的高倍率信息压缩和复原技术，用于印刷照排系统。以后又设计专用的超大规模集成电路实行复原算法，显著改变了性能价格比。这一技术已经领先于国际先进水平，他所领导研制的华光和方正系统开始在全国的报社和出版社使用。

1980 年 2 月 21 日，时任电子工业部长的江泽民同志，写信给党中央，报告王选的研究成果，建议不再向国外进口同类产品。邓小平同志批示表示支持。同年，光明日报在头版头条报导了这一科技成就。1985 年，中央电视台新闻联播也报导了这一消息。印刷业告别“铅与火”的历史，就此开始。

1985 年，方正系统列入全国十大科技发明成果。

1986 年，获日内瓦科技发明奖。

1987 年，获国家科技进步一等奖。

这些成果应该令人满足了，但王选却没有笑起来。他说：“国家

花了这么多的钱，只是得奖却没有创造财富，如何对得起国家和人民？”

方正集团在继续前进。一些关键设备得到不断地改进，输出系统的一项重要设备，王选领导了前五代，年轻博士阳振钟领导了后两代。方正集团的技术研究院副院长、34 岁的邹维发明了包括动画制作在内的一系列新技术。

1992 年 1 月 21 日，《澳门日报》的彩色版用方正激光照排系统排版印刷，轰动海内外。台湾的印刷业同行在报纸上以“眼见为实”加以报导，原来用电子分色机三、四个小时的工作，现在只要 20 分钟，乃至 9 分钟就可以完成。这样的技术是一种“挡不住的诱惑”。现在，台湾国民党的机关报《中央日报》、最大报业集团《联合报》系列、最大发行量的《自立晚报》都已采用方正的激光照排系统。一位台湾人士曾认真地说过，你们大陆的方正技术帮助台湾的国民党机关报，江泽民先生大概会不高兴罢？王选的回答是：“江泽民总书记一定会高兴的”。果然，王选在元宵夜谈到这消息时，江泽民同志非常高兴，认为这是两岸正常的科技交流。1995 年，方正集团股票在香港上市，王选成为名符其实的科学家兼企业家。

现在，方正集团及其伙伴的产品占有国内排版系统的市场份额的 99%，国外市场的 70%以上。计算机技术是西方发达国家领先的领域，中国科学家要在某一方向上占据一个领先地位非常不容易，王选的成功，具有很不平常的意义，其中数学技术是关键的因素之一。

中国的科学家很多，但能赚钱的科学家不多，王选是杰出的一个，他给我们带来的启示是十分深刻的，让我们来听听王选自己的说法。

“科技顶天，市场立地”。王选的这一“顶天立地”说揭示了新时代科学技术发展的一种方向。

“可怕的满足感”。王选提到，在 80 年代初，科技人员最时髦的是出国、写论文、评职称，以为这样就是对国家做贡献，于是就满足了。那时，埋头搞新技术，做没有把握的技术攻关，有了成果也不能发表，没有文章不能升教授，所以那是很不受人欢迎的工作。据说当

时的聂荣臻元帅对如此评教授也忧心忡忡。医生不看病，急着发论文，这种情形，到改变的时候了。

“没有先进水平的填补国内空白是没有意义的”。我们常常见到报导说，某项科技成果达到 80 年代的国际水平，填补了国内的空白。这样的成果只能在展览会上陈列。当外国新产品进来时，“成果”已经是过时产品，除了报废别无用处。这样的科研“从立项之初便注定要失败”，“技术不超前，等于浪费国家资源”。这是何等宝贵的忠告啊！

“知识分子长期价廉就不会物美了”。一位领导人曾说中国知识分子是“价廉物美”。王选说，作为中国知识分子之一，能够为国家作无私贡献，值得自豪。但是，凡事都有一个限度，如果长期“价廉”，就不会“物美”了。

“方正集团要在未来造就 5～10 名院士，几十个百万富翁”。王选说，“知识经济时代，知识更新非常之快。比尔·盖茨也许要在 55 岁退休，我已经 61 岁了，不可能再在技术上领导方正集团，必须交给年轻人，他们做得比我好，这些人中间，应当出现中国科学院和中国工程院的院士。他们所创造的价值，也应该得到应有的回报，成为百万富翁”。

中国未来的数学技术，将会百花齐放。王选的榜样，将会永远激励后来者。

3. 中国的 973 计划

数学是中华民族擅长的学科。因此，中国数学应该而且完全能够率先赶上国际先进水平。发展数学需要数学家的努力，而政府部门的支持则是成功的关键因素。其中，1983 年成立的国家自然科学基金会对中国数学的发展起着十分重要的作用。1989 年，专为发展数学科学而设立的“天元数学基金”，更是国家对数学发展的特别投入，以鼓励数学科学实现“率先赶上世界先进水平”的目标。

1997 年 3 月，国家自然科学基金会提出了我国未来数学发展的

重点课题，为中国数学界指出了努力的方向。这就是著名的“973 计划”。以下是其中的主要部分。

(1) 核心数学

它是数学的核心，应用数学的基础。重要方向有：

- 解析数论、代数数论与代数几何
- 群与代数及其表示理论
- 流形和复形几何学
- 整体微分几何
- 经典分析的前沿问题
- 随机分析和无穷维分析

(2) 非线性问题的数学理论和方法

各门自然科学中的非线性现象和纯粹数学各分支交叉形成的许多生长点。重要科学问题和研究方向有：

- 非线性偏微分方程
- 变分理论和几何分析
- * 动力系统
- 经典和量子系统的数学问题
- 随机系统的数学问题

(3) 金融和高科技中的数学建模、计算和运筹决策

这是国民经济可持续发展、高科技的重大突破和科学管理所面临的重大挑战性课题：

- 数学物理的高性能计算
- 高维流体力学的计算方法
- 数学机械化与现代组合方法
- 高维、定性和不完全数据的统计方法
- 经济和高科技中的统计建模、推断与计算
- 大规模、高复杂性问题的最优化方法
- 高科技中的计算运筹的理论和算法
- 金融财政重点数学问题

(4) 复杂系统的建模、分析控制与优化

- 复杂系统的建模
- 随机系统的控制和适应控制
- 非线性现象的分析、控制与应用
- 无穷系统的控制
- 复杂系统的优化与控制
- 复杂系统分析与可靠性
- 大规模多层次系统的优化理论和方法

从以上的清单可以看出,中国数学的发展已经进入新阶段,许多从前没有听说过的课题进入了我们的视野。

数学正在改变,数学观也真的是变了,让我们共同努力,把我国建设成 21 世纪数学大国!

第五节 “推测数学”可否存在

20世纪的数学正在一日千里地向前发展,所谓“第三次数学危机”,不过是哲学家们故做的惊人之语。但是,数学界内部也并非风平浪静。1993年7月,美国数学会的《公报》上发了一篇文章,题为“理论数学——数学和理论物理的文化综合”[2]。作者是美国哈佛大学的贾弗(Jaffe)和弗吉尼亚理工学院的奎因(Quinn)。一篇文章本不算什么大事,令人惊奇的是一大批世界顶尖的数学大师就此发表看法。他们的观点不尽相同;可都从各个侧面反映了对传统数学观的挑战。争论的主题是:没有严格证明的推测性的数学结果是否允许发表?众所周知,数学界历来以数学的绝对严格而自豪,断言数学的严格性是数学的生命,不容许有任何含糊不清和讨价还价。现在居然讨论起无需证明的“推测数学”,岂不是对传统的背叛?这场论战涉及数学科学的深层次问题,其意义似不可小看。在今天跨世纪的国际科学竞争中,这一问题或许会具有重要的战略意义。

1. 分　　工

贾弗和奎因在上述论文里,首先将数学和物理学进行类比。在物理学中有理论物理和实验物理的分工。大约从1900年开始,相当多的物理学家只做理论研究,对物理现象作各种理论推测。另一部分实验物理学家则通过实验证实或推翻各种推测。在数学界,一位数学家要取得一项创造性的成果,也必须先进行猜想和推测,然后再通过严格证明以验证其推测是否正确。这表明数学界还没有出现像物理学界那样的分工,数学家必须承担“推测”和“验证”双重任务。

于是贾弗和奎因建议:应该允许“推测数学”的存在,在杂志上发表未加证明的“推测”性的数学论文,及早完成“理论数学”和“证明数学”的分工。

2. 背　　景

贾弗和奎因的论文的出现,有其特定背景。1990 年,国际数学家大会在日本京都举行,会上有 4 人获 4 年一届的世界数学最高奖——菲尔兹奖,其中的一位是物理学家威滕(E. Witten),这是没有先例的。威滕的主要贡献是利用物理学的观点和方法,提出了一系列数学新见解,得到许多数学新结果。他给出的一种数学不变量,恰好和另一位菲尔兹奖获得者琼斯(Jones)的工作——扭结的琼斯多项式相联系,在数学界引起轰动。理论物理学家从物理学需要提出的数学猜测,内涵十分丰富。因此,尽管这些物理学家并未经过严格数学训练,所作推测却很有道理。接着,许多数学家极有兴趣地对这些推测进行严格的数学证明,便形成了一个个数学热点。可见,威滕等物理学家已经做出了第一流的“推测数学”工作,而一批数学家则从事艰巨的“证明数学”工作,对推测加以验证,分工实际已存在。

数学和物理学联系历来很密切,有一门学科就称为数学物理,但二者间的关系却不大融洽。许多物理学家认为数学家是无用的苛刻的理论家。诺贝尔物理学奖获得者费曼(R. Feynman)常常取笑数学家不愿采用那些“管用”但不严格的数学方法[3]。连十分重视数学家的杨振宁也说过:“有些数学书,搞物理的只看了第一页就不想看了。”[4]

3. 传　　统

数学界崇尚逻辑演绎绝对严密的格局是在 19 世纪末、20 世纪初逐步形成的。牛顿发明的微积分,欧拉的大量数学发现,以及中国古代数学成果,以现今的观点看,都是不严格的,却无损于它们的历

史光辉。

数学界也有许多成功的猜想,如费马猜想、黎曼猜想、哥德巴赫猜想,以及希尔伯特提出的 23 个数学问题,都是成功的事例。这些猜想只提出一个目标,如能解决,功劳归于证明者。有些猜想附有一些基本想法,有一个纲领和计划,如韦尔(Weil)猜想、朗兰(Langlands)纲领、森(Mori)计划等。当前数学界还有"若 A 真,则 X、Y、Z 也真"的研究,大兵团作战(如有限单群)的计划,一项基金下的分工合作等。这些也在某种程度上规划了未来研究的目标,也是一种猜想。此类工作是受到赞扬的。

然而,另一些未加证明的猜想性研究工作则举步艰难。20 世纪初的意大利代数几何学派,以大量猜想为依据所做的工作,未被数学界承认;1895 年,庞加莱的《位置分析》是代数拓扑学的开端,但这篇"引人入胜又令人恼火的作品"完全是直觉的,所以在二十年内一直被冷落;汤姆(R. Thom)在 1958 年以前做的是严格的数学工作,因而得了菲尔兹奖,但此后完成的奇点理论和拓扑稳定映射的工作,则不甚严格,建筑在其上的"突变理论"及其各种应用,更有争议。

总之,尽管我们对牛顿发明微积分的不严格工作推崇备至,却不能容忍今天的任何"不严格的证明",即使看起来它很具创造性。

4. 赞　　同

阿蒂亚(M. Atiyah)是当代最负盛名的数学家之一,也是牛顿之后任三一学院院长的唯一数学家。他对贾弗和奎因文章的观点表示赞同,认为"把基于不严格证明的数学和基于启发式的数学加以区别是特别重要的"。数学要具有活力,出现激动人心的新局面,就不得不允许新思想和新方法的探索,今天我们对证明有高标准要求,但在早期发展过程中,我们必须准备做更多的冒险。直觉的启发式的物理论证建立的大量工作,乃是欧拉和拉马努杨的现代事例。

事实上,量子场论和几何的整个领域按这样风格产生了很有价值的新结果。许多重要情形用其他方法已有了严格证明,这从另一

面说明直觉式的证明往往率先发现新结果。原本不严格的费曼积分，现在已用组合学和代数学技巧给出了严格的含义。威滕基于狄拉克算子和超对称形式化给正能量猜想以非常简单的证明。丘成桐的证明是可尊敬的，但威滕的成功也不可否认。

数学中猜想的价值有时要超过证明。以霍奇(Hodge)(阿蒂亚的导师)的调和形式大纲为例，霍奇自己的证明本质上是错的，因为他用的分析工具不合适。后来的证明采用了更好的分析方法，但这无损于霍奇的光荣。物理学家在第一线作研究探索时很少考虑数学的严格性，而数学家能给出严格证明的结果很少属于物理学热点。现今几何与物理学前沿的发展，是 20 世纪数学最令人耳目一新的事件，它将会制约 21 世纪的数学。

年轻一代将会追随这一趋势，但正如贾弗和奎因所警告，对于那些想稳稳当当获取博士学位的年轻人，这会是过于冒险的。

5. 反　　对

麦克莱因(S. Maclane)是数学权威人士。他在评论贾弗和奎因的文章时说："他们作了一些有趣的考察，然而，在我看来，他们的主要建议是危险的，也是错误的。"

麦克莱因首先回忆 1982 年秋在沙特阿拉伯的一家旅馆开会时，和阿蒂亚的讨论，题目是：数学研究是如何作出的。麦克莱因认为，代数学研究意味着首先要获得和理解必须的定义，看看能算出什么，能推出什么，最后得到具有新结构的定理。对阿蒂亚来说，研究几何学意味着对一些模糊的、不肯定的情景苦苦思考，看看能发现什么，最后才达到定义、定理和证明。这两类数学家具有不同的思考路线，但他们的共同标准是最后得到经严格证明的定理。

数学的理解链是"直觉——尝试——出错——推测——猜想——证明"。物理学已经提供了许多很好的建议和新颖的直觉，但数学无需去模仿"实验物理"的风格。麦克莱因说："数学依靠证明，证明是不朽的。"

6. 自　白

汤姆是突变理论的创立者。他表述了自己关于数学严格性的态度："1958 年以前，我生活在以布尔巴基学派人士为主的圈子里，即使我有一些不严格之处，其他人，嘉当(Cartan)、塞尔(J. P. Serre)、惠特尼(Whitney)会帮助我保持一种人们可以接受的严格标准。但自 1958 年获得菲尔兹奖之后，我就按照我自己的自然趋势走下去……几年以后，我成为格罗森迪克(A. Grothendick)的同事，竟使我觉得严格性并非数学思维的必要品质。"此后，汤姆的许多重要工作在初次发表时都是不严格的。当然，后来许多人关于奇点理论的阐述则是严格的。

"因此，贾弗和奎因的文章涉及了非常重要的问题"，汤姆认为这是第一次有机会深入讨论数学严格性问题。严格是相对的，不是绝对的。它依赖于读者已有的和被期望的应有的背景，这是一种局部的、社会学的准则。

"严格性是一个拉丁名词。我们会想起僵死(rigormorits)，即僵化的尸体。我要把数学分为以下的三类：

第一，以婴儿摇篮为标记。这是'活的数学'，允许改变、澄清、完成证明、反对、反驳。

第二，以十字架为标记。这是坟幕上的十字架。作者声明它已完全严格，具有不朽的正确性。这类工作将构成'坟墓数学'。

第三，以教堂为标记。这是外部的权威，由高级教士组成，判断哪些工作确已成为'坟墓数学'。"

汤姆在这里用半开玩笑的态度，诉说着一个严肃的话题。

7. 嘲　弄

分形数学的创始人曼特勃洛托(B. B. Mandelbrot)发出了对当代流行的数学准则的猛烈抨击。他愤世嫉俗的看法令人吃惊。曼特

勃洛托把今天的数学家嘲讽地称为查尔斯数学家(Charles Mathematicians),因为美国数学会(AMS)位于查尔斯大街上。他不同意贾弗和奎因文章的观点,是因为嫌他们走得不够远,指责贾弗和奎因想在查尔斯数学家内部建立“警察国家”,并使这种次序越过数学边界以至成为“世界警察”。贾弗和奎因的文章说“文学系的学生通常具有反数学的观念……常常否认他们的工作是不完备的”。为了改变这种情况,贾弗和奎因不是用平等地进行协商的办法,而是开“处方”(用贾弗和奎因自己的说法)。曼特勃洛托说:“为什么科学家们要理会‘查尔斯数学家’的荣誉,给‘查尔斯数学家’恶劣的记录以荣誉呢”?

安德森(P. Anderson)把数学严格性看成“不相干的和不可能,也无关紧要和令人烦恼”。以数理统计为例,内曼(J. Neyman)曾训练他的追随者要做到极端严格(他们的工作只是为了使查尔斯数学家感兴趣)。但现今内曼的影响已消退,情况变了,数理统计被解放出来,找到了自己的科学位置。如果现在把贾弗和奎因的处方用于数理统计,它将再次走进死胡同。

曼特勃洛托说:“我读数学史的体会是,人类在不断产生具有最高数学天才但不屈服于类似贾弗和奎因处方压力的人物。如果真的施加压力,他们会离开数学。这对每个人都是莫大的损失。”他的第一个例子是概率论大家利维(P. levy 1886—1971)。法国式的查尔斯数学家谴责他不能充分证明定理(包括有时会出现初等计算错误)。利维虽无法逃出查尔斯数学家的手掌,但不屈服,直到70多岁时仍有极好的惊人的直觉工作问世,那些“不完备的”事实不断为大家提供极有价值的工作。但在他71岁时(当时曼特勃洛托是和他共事的初级教授),仍被禁止教概率论。对他的折磨是令人难以想像的。

第二个例子是庞加莱(H. Poincare)。在最近公布的厄米(Hermite,庞加莱的导师)给米塔格-莱弗勒(Mittag-Leffler)的信中,有多处抱怨庞加莱把要他修正并发表充分证明的劝告当做耳边风。鉴于庞加莱不可救药,厄米和皮卡(Picard,庞加莱的继任导师)竟然不让

庞加莱教数学,只让他教数学物理和天文学。庞加莱编写的讲义包括基础光学、热动力学、电磁学(二、三年级的理论物理课程)。庞加莱在 1895 年写的《位置分析》一书确实在很长时间内成了"死区"。曼特勃洛托说,请问:受害的是谁?难道要庞加莱屈服于厄米和他的后继者,等他知道如何走出那个"死区"再来出版这本名著吗?

曼特勃洛托主张改善数学和临近学科的关系,认为最好的边界是开放的边界,即允许名义上的物理学家以其数学成就受到称赞,而名义上的数学家以他们的物理成就获得褒扬。

8. 理解和证明

菲尔兹奖获得者瑟斯顿(W. Thurston)写了一篇长文来回应贾弗和奎因的文章,题目是:数学中的证明定理。文中介绍了数学家如何推动数学的发展,如何增进人类的数学理解,论述非常深入和吸引人。如他列举人们对导数的几种理解:从无穷小变化率到纤维丛的联络,揭示人类语言、符号、逻辑、视觉等在做证明和交流证明中的作用。这些论述具有特殊的哲学意义,但并非直接回答贾弗和奎因的论文。

在谈到什么是证明时,瑟斯顿说:"当人们做数学时,主要依据意识流和社会的正确性标准,很少考虑形式化的书面文件。人们常常不善于检验形式证明的正确性,却会发现证明中潜在的弱点和缺陷。"瑟斯顿赞成现今通过的严格性标准,认为这是保证数学完全可信的基础,但也认为人们不能依靠形式化来做数学。

瑟斯顿自己的经历和"推测数学"有些关联。他的两项重要工作,一是建立叶状结构理论,二是用几何观点研究三维流形。在 70 年代末和 80 年代初,他的工作不能被人理解,一些数学家认为那是不可靠的。对此,瑟斯顿解释说:"我的数学教育有自己的独立性和习惯。有很多年我是自学的,按照我个人的思维模式去思考数学。这对我思考数学带来许多好处,但是,我能自由地和自然地运用某些概念,对大多数数学家却是陌生的。这造成了我的数学思想和别人

交流的困难。"事实证明,瑟斯顿的数学工作是正确的。许多数学家陆续用通常使用的概念和方法证明了他的许多论述和猜想。

9. 启　　示

参加这场讨论的还有博雷尔(A. Borel)、蔡廷(G. J. Chaitin)、弗里丹(D. Friedan)、格里姆(J. Glimm)、格雷(J. J. Gray)、赫希(M. W. Hirsh)、吕埃勒(D. Rueile)、施瓦茨(Schwarz)、乌伦贝克(Uhlenbeck)、威滕、塞曼(C. Zeeman)。以上诸多名家,意见虽不尽相同,但多半赞同贾弗和奎因所提出的问题,认为值得讨论。20 世纪刚刚过去,这场讨论是否会给未来世纪的数学发展规律带来革命性转折,值得重视和研究。

中国现代数学是 20 世纪才发展起来的,经过几代人努力,已获得世界性成就。在中国科学事业中,数学正计划率先赶上国际先进水平,表明我国数学研究队伍已具有追赶世界数学强国的实力。但许多数学界知名人士也认识到,中国数学在整体上仍和国际先进水平有相当大差距。如果说我们在数学技巧、证明难度上还比较强的话,那么,在数学创意、新理论建立、新学科奠基方面,则有很大距离。如此考虑,也许"推测数学"的提出,正击中我们弱点。我们常见我国数学家解决外国人的猜想,却几乎没有听到中国人有过什么重要猜想。这固然是中国数学还没有那么大名气,即使有了猜想别人也不重视,但另一方面,我们确实站得不够高,直觉的洞察力不够强,因而提不出有价值的猜想。

当然,"推测数学"的讨论并不意味着数学可以随意猜测,有价值的推测一定要建立在严格训练的基础上。此外,对有创意的数学工作,则应允许在个别地方出点错,有些不严密,不要吹毛求疵,弄得人们谨小慎微。应当鼓励推测,经过讨论,也许就成了有意义的创造。在这方面,我们的环境不能说很宽松。

令人担忧的是中国的数学教育,中学生负担之重,数学想象几乎被题海淹没,无暇看课外数学书,无从汲取新鲜数学思想。教学方法

也是以记忆题型为目标，以形式上的严谨为准绳，把生机勃勃的数学思想阉割得支离破碎、面目死板。许多数学教育界人士则片面追求升学率。“万丈高楼平地起”，只有从中小学起就培养学生数学创新意识，中国才能真正成为数学大国。

参考文献

[1] Jaffe A, Quinn A. Theoretical Mathematics: Toward a culture synthesis of mathematics and theoretical physics, Bull Amer Math soc, 29(1):1, 1993.

[2] Bull Amer Math Soc, 30(2):159—211, 1994.

[3] Feynman R P. Surely you're joking Mr. Feynman. Adventures of a currious character. New York: W. W. Norton, 1985.

[4] Zhang D Z, C N Yang and Contemporary Mathmatics, The Methematical Intelligencer, 15(4):13, 1992.

第六节　数学的统一性

数学本来是统一的。古希腊出现了算术、代数、几何的区分，但所有数学家三者都研究。欧几里得的《几何原本》，其中含有算术和代数的内容。牛顿和莱布尼兹发明微积分，出现了分析学。自此，代数、几何、分析三足鼎立。一些大数学家，如欧拉、柯西、高斯、黎曼、希尔伯特等都是全才的数学家。到 20 世纪，能够通晓全部或大部数学的名家渐渐减少，50 年代逝世的 H·外尔、冯·诺依曼也许是最后的两位。

20 世纪下半叶，数学科学迅猛发展，数学分支如雨后春笋，科目越分越细。现在美国《数学评论》中，数学分支的分类目录共 65 大类，500 小类[1]。著名的数学家也许可以涉及其中的几个大类，而多数数学家也许只是一个大类中的若干小类的专家。隔行如隔山，一篇普通的数学论文，愿意去读又能够读懂的人，恐怕只有几个人或者几十人。那么，数学的统一性，在 21 世纪还能保持吗？这是一个严峻的问题。以下是几位数学家的观点，可以说代表了当今数学界的主流看法。

阿蒂亚(Michael Atiyah, 1929—　)，20 世纪下半叶影响最大的数学家之一。1990 年，他以数学家的身份，当选为英国皇家学会会长、剑桥三一学院院长，以及牛顿数学研究所所长。这种集三职于一身的情况，是牛顿以来的数学家所未曾有过的荣誉。1974—1976 年，阿蒂亚担任伦敦数学会主席，他的就职演说题目是：数学的统一性。他在演讲中举了三个例子：代数方面的高斯整数环 Z[$\sqrt{-5}$]，几何方面的麦比乌斯(Mobius)带，分析方面的由核函数 $a(x, y)$ 确定的线性微分—积分方程。这三个似乎彼此无关的内容却具有深刻的

内在联系。麦比乌斯带的存在和多项式环 $R[x, 1-x]$ 的因子分解不唯一性相联系。如果核函数满足 $a(x, y)=-a(y, x)$，则上述的微分一积分方程相当于斜伴随算子 A。然后可以看到 A 的奇偶性恰和麦比乌斯带的拓扑性质相一致。阿蒂亚总结这些联系之后说道：

“在我看来，这种相互联系决不是一种偶然的巧合，实际上反映了数学的本质。……在数学范围内，其内在的雷同性也应该凸显出来，就没有什么值得奇怪的了。我感觉有必要强调这一点，是因为在公理化时代，人们倾向于把数学分为专门的分支，每一分支只局限于从给定的一套公理推演出一些结论。我并不完全反对公理化方法，但只能将它当做一种方便的措施，以便集中处理我们的对象。我们不能把它的地位抬得太高。”

“数学的统一性和简单性都是十分重要的……。如果我们所积累起来的知识要代代相传的话，我们就必须不断地努力把它们简化和统一。”[2]

芒福德(David Mumford, 1937—　)是1994—1998年度的国际数学家联合会主席，1974年的菲尔兹奖获得者，美国布朗大学教授。他是一位纯粹数学家，专长代数几何。1997年，芒福德在庆贺他60岁生日的学术会议上发表了一次演讲，内容涉及未来数学的发展[3]。这里是根据他的讲演摘录整理的一些观点。

首先，“我们能否在所有数学学科之间保持相互交流的传统，并能否抵御数学越来越专门化的趋势？”数学的进展，使得数学家很难在一个以上的领域内处于顶尖地位，更不要说要掌握整个数学了。但是，我们还是应该有所作为的。最近，大学一年级的化学课从一开始就引进量子力学的思想，令人震动。

数学界有国际数学家联合会，每4年举行一次国际数学家大会(ICM)，在大会上有10多个大会报告，100多个分组报告，而且分成19个小组进行学术交流。这是一个非常值得珍视的传统。这表明数学还是一个统一的整体。但是，与数学近邻的物理学、计算机科学则不是这样。物理学界有一个国际联合会，但是没有全球性的物理

学家的大会。物理学界已经分裂,实验家和理论家之间,基本粒子和凝聚态统计力学的研究者之间,数学物理学家和“真正”物理学家之间,没有汇聚起来报告各自进展的需求。计算机专家则连一个国际性的组织都没有。确实,要把各种不同领域工作的学者汇集在一起,不是一件容易的事。专门知识有一种分裂的自然倾向。一旦分裂,就出现自己的分机构。然后独立发展,彼此互不通气,思想传播的速度放慢,重复工作增加,这对科学的整体发展当然是不利的。那么数学家为什么会来参加4年一届的国际大会呢?答案是:在具有共同的工具和洞察力的意义上说,数学仍是单一的学科。ICM是交流深刻洞察力和理解数学思想的极好机会。

数学家在传播数学思想的时候,有一个特殊的习惯:以“充分一般的”方式陈述结果,必须建立起一套有关定义和抽象概念的完整天地。于是,原始的例子不见了,数学家像学徒一样从头学起,把每个细节都搞清楚。这种要求大约是在30年代的布尔巴基学派开始并加以固定的。这意味着,数学家只要在一个抽象概念的集合上工作,经过一段学徒生涯就会成功。可是,我们真要一辈子“住”在布尔巴基的屋子里吗?英国的著名数学家M·阿蒂亚爵士说,一个新思想最有意义的部分,常常不在那些最一般的深刻定理之中,而往往寓于最简单的例子、最原始的定义,以及最初的一些结果。最重要的信息却常常包含在容易的部分,甚至在几个简单且深刻的观察之上。这些思想可以而且应当在国际数学家大会上进行交流。

其次,“我们要定理还是模型”?

做数学的目的是什么?一般都认为是“提出和证明定理”。定理,也只有定理,才是这个领域的流通货币。它可以为你买到学位,得到发表演讲的邀请的机会以及一份好的工作。那些了不起的大段的证明往往有一种神秘感。在每个漂亮而深刻的证明后面是一部“上帝的书”。纯粹数学家的特征之一是孤军奋斗,努力把一团乱麻似的思想和论断梳理清楚并组织得有意义。这足以引起所有人的同情和怜悯。

和定理证明不同的是做数学模型。在应用数学里,模型在表达

问题的本质上有非凡的作用，即能把实验的无序状态转化为明确有序的数学问题。此外，纯粹数学也需要模型。50 年代的代数拓扑就是这样的：先定义空间的同伦型范畴，然后构造一类拓扑空间的模型，一个领域就爆炸性地发展起来了。

因此，创建好的模型和证明深刻的定理一样有意义。承认这一点，数学将会得益。“模型”和“定理”都应该在学位、讲座、工作、晋升等方面获得同样对待。

与定理和模型的情形一样，纯粹数学和应用数学之间也有很多争论。其实，一个好的数学课题往往是在纯粹数学和应用数学之间跳来跳去，不能严格分开。我们需要使数学科学的所有领域都获得应有的地位。例如，有的论文只讲某模型的理论分析，却不指出其实际来源，特别是在指出来源会明白问题应如何简化及可能出现的变化时，硬要“纯粹”地表述，那是一种虚伪。

最后，应当指出，数学是很难作出规划而加以发展的，应当允许个人的探索。我们应当时常反复思考，如何把自己的成果向别的领域的专家们介绍清楚，每个发言者都要考虑听众的需要。我们也必须愿意从别的领域中寻求启发，无论它是纯粹的或者是应用的。

L·罗瓦兹(L. Lovasz)原籍匈牙利，现为美国耶鲁大学教授，著名的组合论专家，国际计算机科学界的领袖人物。他认为“数学是一个整体，数学的分化决非自然结果”。以下是罗瓦兹的一些见解。[4]

数学已被许多分界线割裂得支离破碎。听凭这种现象蔓延，必将导致可悲的结果。我们必须竭尽全力填补这些鸿沟。

填补鸿沟以改变这种状况的外部条件有三：第一是数学研究规模迅速增大，正如人口密集，需要增加交通设施那样，数学的统一指挥、互相交流在日益扩大，电子信件、网络会把大家联结在一起；第二是新的应用领域在扩大，生物、金融、计算机科学、密码通讯等领域需要数学，数学家必须合作交流，才能解决这些新问题；第三是新的工具——计算机，乃是对付信息爆炸的有效工具。人们阅读书面论文时，并不逐行阅读，网上浏览交流会更直接。因此，我们对数学的统一性应该抱有信心。

罗瓦兹特别提到表现数学研究成果的方式。目前的通用形式是:定义概念,给出定理,予以证明。但是,随着信息交流的扩大,数学活动的需求也在改变。新形式包括:撰写综述论文,提出问题和猜想,收集实例,报告实验结果等等。

对于新的附有严格证明的论文,可读性很差,往往没有人能全部读懂,所以现在普遍欢迎综述性的论文。出版界也喜欢大部的综述论文,而不愿出论文集。对于综述论文,我们往往有偏见,看不起,认为那不是创造,和作者的成就不挂钩。其实,综述论文是保持数学统一,维护数学团结的重要手段。我们应当向人文科学界学习,他们有评判优秀综述论文的标准。

问题和猜想也应该拿出来交流。要把提出好的问题和猜想看成为一种科研成果,甚至是高超的艺术。这是创造的开始(参见本书"'推测数学'是否允许存在"一节)。

罗瓦兹就有限与无限,确定与随机,连续与离散等的统一性作了阐述。

综上所述,数学的统一性将是数学界继续关注的焦点。让我们把"一个数学整体"带入新世纪。

参考文献

[1] 美国数学会. 数学分类目标. 1991.
[2] 阿蒂亚. 数学的统一性. 江苏教育出版社,1995.
[3] D. Mumford. 数学的趋势. 中国数学会通讯. 总第 68 期,1998 年 12 月.
[4] L. Lovasz. 数学是一个整体. 上海数学会通讯. 总第 8 期,1998.

第二章

现代数学专题选讲

第一节　谈无限:集合和基数

1. 集 合 与 悖 论

在一般的教科书中,通常用描述性的"定义"来说明集合这个概念:

集合是具有一定性质的事物的全体。

但这不是一个精确的定义。因为什么叫"事物",什么叫"一定性质",什么叫"全体",含义都没有严格界定。当然,在大多数情况下,这并不妨碍我们正确地应用"集合"这个概念及集合的性质来解决一些问题。在应用集合概念和理论的时候,我们要求集合有所谓的"一义性":

即对于任何一个事物 y 和任何一个集合 B,"y 是集合 B 中的一个事物"与"y 不是集合 B 中的一个事物",必定有一个断言而且只有一个断言是正确的。

如果我们用 $x \in A$ 表示"x 是集合 A 中的一个事物",用 $x \notin A$ 表示"x 不是集合 A 中的一个事物",集合的"一义性"要求用数学符号表示,就是

$y \in B$, $y \notin B$ 中有且仅有一个表达式成立。

因而,在一般情况下,集合的界定是很清楚的。然而在某些情况下,按上述描述性定义规定的集合概念会产生麻烦。如:

(1) 理发师悖论

理发师说:他给一切"不给自己刮脸的人"刮脸。

初看起来,理发师的服务对象组成了一个集合 B。但是在讨论

理发师自己是否属于 B 时却出现了矛盾。理发师若不给自己刮脸，他就应该属于 B，即自己也成了自己的服务对象，他就应该给自己刮脸。这样，他就属于"给自己刮脸的人"，从而他就不属于 B。但是若他不属于 B，即他"给自己刮脸"，他自己就不是服务对象，他就不应该给自己刮脸，因而也产生矛盾。这样，若记理发师为 y，则 $y \in B$ 和 $y \notin B$ 都不对。

这样的悖论还有许多。

(2) 语义悖论

由于英语中的音节只有有限多个，因而英语中包含的音节数少于 40 个的英语表达式也只可能是有限多个。特别地，用这样的表达式能表示的正整数也只可能是有限多个。我们用 B 表示"能用这样的表达式表示的正整数全体所组成的集合"。设 x 是用少于 40 个音节不能表达的最小正整数，即 $x \notin B$。但是 x 可以用下面的英语表达式表示：

The least positive integer which is not denoted by an expression in the English language containing fewer than forty syllables.

上述表达式只含有 37 个音节，因而 $x \in B$，与 $x \notin B$ 矛盾。

鉴于以上类型例子的矛盾，数学家重新研究了集合论的基础，尝试用各种方法来避免悖论。他们提出了集合论的公理系统，其作用是对作为数学研究对象的集合加上一定的限制，使之得以消除产生悖论的可能。在这些限制下，上述种种"集合"都被排除在数学研究的对象之外。当然这些限制也是非常宽松的，足够保留数学理论所有有价值的东西，足够满足数学发展的需求。在这样的公理化理论中，集合这个概念仍然不加定义，但是它的性质就由所谓的"集合公理"反映出来。而对集合论基础的研究，导致了数学的一个重要分支——数理逻辑的迅速发展。

2. 集合的基数

对一个集合，我们通常会关心其包含的事物，即包含的元素的多

少。如果集合内的元素是有限多个，此时称集合为有限集。对有限集，我们自然用其所含元素的个数来作比较。此时，我们也把集合内元素的个数称为集合的基数。如果一个集合内的元素有无穷多个，我们如何来定义集合的基数呢？我们又如何来比较两个无穷集合所含元素的多少呢？

为此，我们先分析一下在有限集的情况下，两个集合内的元素的多少是如何比较的。

古代的主妇就知道，如何判断客人的数目是否和椅子的数目相同：如果每个客人坐一把椅子，而每把椅子上都坐了一个客人，不同客人坐的椅子也不同(即没有两个客人合用一把椅子)，则客人数目就和椅子的数目一样多。对于两个集合 A 和 B，我们也可以用下面类似的方法来说明它们所含元素一样多。

设法规定一个将集合 A 中元素和集合 B 中元素的对应方法(这种方法随集合的不同而不同，例如上面的例子中把客人和他坐的椅子作对应)，在这种对应方法下，满足：

1) 对 A 的每一个元素，B 中有一个元素和它对应；

2) 反过来，对于集合 B 中的任意一个元素，总可以找到 A 中的一个元素和它对应；

3) A 的元素不同，B 中对应元素也不同。

这时我们就可以认为，集合 A 中的元素和集合 B 中的元素一样多，称 A 和 B 有相同的基数。

对于有无穷多个元素的集合，先来看如下两个例子。

(1) 普通旅店和客人

设想一个普通旅店，各房间依次编了号码：

$$\#1,\ \#2,\ \#3,\ \cdots,\ \#n$$

现在住进了一批客人。每人住一个房间，没有两个人住同一间房间。如果还有房间没有客人住，我们可以断言，房间数比客人数多；如果这样分配完客人后，发现没有空房间多余，即每个房间都有人住，则房间数和客人数相等；如果这样分配房间后还有客人未住进

去，则客人数多于房间数。

对于有无穷多个元素的集合，会有一些不同寻常的性质。

(2) 希尔伯特旅店

设想一个有无穷多个房间的旅店。各房间依次编了号码：

#1, #2, #3 …

现在来了一个代表团，有无穷多个成员。为管理方便，团长为每个成员编了号：

1, 2, 3 …

代表团到达旅店后，团长让每个人住进号码相同的房间：编了1号那个人住进#1房间，编了2号那个人住进#2房间，…我们发现房间和代表团成员一样多：因为每个人有一个房间住，而每个房间都住了一个人，没有房间空着。这样，代表团成员的数目和旅店房间的数目相同，我们可以称代表团成员的基数和旅店房间的基数相同。

设想等代表团安顿好后，又来了一个人。他是否也能住下来呢？答案是肯定的：我们让他住进#1房间，让原先的1号移到#2房间，2号移到#3房间，其余的人都依次移到下一个房间。于是客人总数和房间仍然一样多。

现在我们把这个性质描述为自然数集合1, 2, 3, …的性质。给房间编号事实上是确定了把旅店的房间和自然数对应的一种方法。因为每个房间都有一个号码，而每个自然数是某一个房间的号码，不同的房间号码也不同，因而旅店房间的集合和自然数集合有相同的基数。我们用 N 记自然数集合1, 2, 3, …则上面的情况提示我们，往自然数集合内加一个元素后，所得到集合的基数仍然是 N，即

$$N+1=N$$

同样，如果此后又来了100个客人，我们请原先住#1房间的客人移到#101房间去，住#2房间的客人移到#102房间去，…所有其他的人都往后移100个房间。将让出来的100个

房间安排新来的100个客人住。这时房间数仍然和客人数一样多，用前面的记号，有

$$N + 100 = N$$

实际上，用相同的方法我们可以证明，对于任何一个自然数 p，都有

$$N + p = N$$

更有甚者，如果后来又来了一个有无穷多个成员的代表团，成员们由他们的团长编了号码：

$$1,\ 2,\ 3,\ \cdots$$

我们仍然可以安排这个代表团住下来。安排的方法是这样：让原先住＃1房间的人移到＃2房间，让原先住＃2房间的人移到＃4房间，…让原先住＃100房间的人移到＃200房间，…于是将腾出来的单数号房间依次安排新来的代表团成员住。这样我们得到

$$N + N = N$$

我们再来看由满足不等式 $0 < x < 1$ 的一切有理数 x 所组成的集合，即区间 $(0,\ 1)$ 内的有理数全体。初看起来，$(0,\ 1)$ 内的有理数相当多，因为任何两个有理数之间有无穷多个有理数，即有理数在 $(0,\ 1)$ 内是稠密的。但是我们可以证明，在区间 $(0,\ 1)$ 中的有理数和自然数一样多。证明的方法是这样的：

因为 $(0,\ 1)$ 内的每一个有理数可以唯一表示为

$$\frac{q}{p} \quad (p > q,\ p、q\ 互素)$$

此处 p 和 q 都是自然数。我们可以按照先排分母后排分子的方法把 $(0,\ 1)$ 内的所有有理数排成一列，去掉那些分子、分母不互素的那些分数：

$$\frac{1}{2}$$

$$\frac{1}{3}, \frac{2}{3}$$

$$\frac{1}{4}, \frac{2}{4}, \frac{3}{4}$$

$$\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}$$

$$\cdots$$

按照这样的方法，(0, 1)中的每一个有理数都可以在这个序列中找到自己唯一的位置，即每个数都有自己的位置号码。另外，这个序列又显然是无限长的$\left(\text{因为形如 } \frac{1}{k}(k > 1) \text{ 这样的有理数必在序列中}\right)$。事实上我们把它们组成了一个编了号码的代表团。由前面的分析，(0, 1)内的有理数集合有基数 N。

那么有没有一个集合的基数比 N 更大呢？或者说，有没有一个含有比自然数更多元素的集合呢？

答案是肯定的。我们可以证明(0, 1)内一切实数所组成的集合的基数比 N 大。现在来证明这个事实。

(0, 1)内的实数都可以表示为一个无限的小数：

$$0 \cdot q_1 q_2 \cdots$$

这里的 q_1，q_2，…是 0—9 中的一个数字不全为 9，且不以 0 为循环节。反之，任何一个用这种形式表示的小数也一定在区间(0, 1)内。假如(0, 1)中的实数的基数和自然数的基数相同，都为 N，则我们一定有一个方法可以将它们和自然数对应起来，即可以给它们依次编号。我们把第一个数记为 a_1，第二个数记为 a_2，…，等等，把它们依次写出，就是：

$$a_1, a_2, a_3, \cdots$$

现在我们来作一个小于 1 的实数 r:小数点后的第一位与上面的第一个数 a_1 的第一位小数数字不同。例如,假设第一个数是 0.123 456…则 r 的小数点后的第一位小数取 2 或 3 等等。r 的第二位数字和第二个数 a_2 的第二位小数的数字不同。依次可以得到 r 的任何一位小数位上的数字,这样也得到了 r。从 r 的构造方法可知,r 是(0, 1)内的一个实数。但是 r 却没有被编号:因为任何一个已编号的实数和 r 至少在一个小数位上的数字不同。

如果我们把(0, 1)的基数记作 R,则 R 要大于 N。R 称为连续统的基数。

3. 模 糊 集 合

集合的一个基本性质是"一义性",即对于任何一个事物 y 和任何一个集合 B,"y 是集合 B 中的一个事物"与"y 不是集合 B 中的一个事物",必定有一个断言而且只有一个断言是正确的。但是在实际生活中,许多现象中不会这么绝对化。

例如,一个人是否属于"年轻人"集合是很难准确界定的。90 岁的人肯定不年轻,20 岁的人肯定年轻。但 30 岁的人是否年轻? 35 岁、40 岁的人是否年轻? 这时我们很难用"要么属于年轻人范围,要么不属于年轻人范围"这样绝对的断言下结论。

又如,在历史研究中,奴隶制社会和封建制社会之间有一段历史的过渡时期。殷商是奴隶制社会,秦汉以后是封建制社会,这是肯定的。而对处于春秋战国时代的诸侯国,我们却无法在"属于奴隶制社会"或"属于封建制社会"之间作一个断然的抉择。

为适应于这种情况,数学家引进了模糊集的概念。一个元素 x 是否属于一个集合 M 用隶属度(或称隶属度指标)$\mu_M(x)$来描述。隶属度要符合下面的规定:

当 x 属于 M 时: $\mu_M(x) = 1$,

当 x 不属于 M 时: $\mu_M(x) = 0$,

其余情况下 $0 < \mu_M(x) < 1$。

例如，规定一个年龄为 x 岁的人属于年轻人集合 Y 的隶属度为

$$\mu_Y(x) = \begin{cases} 1 & 0 \leqslant x \leqslant 25 \\ \left[1 + \left(\frac{x-25}{5}\right)^2\right]^{-1} & x > 25 \end{cases}$$

上述公式中第一式的含义是，年龄在 25 岁以下的人恒可看作是年轻人。根据上述公式计算，30 岁、35 岁、40 岁、50 岁的人属于年轻人集合 Y 的隶属度分别为：

$$\mu_Y(30) = \frac{1}{2}$$

$$\mu_Y(35) = \frac{1}{5}$$

$$\mu_Y(40) = \frac{1}{10}$$

$$\mu_Y(50) = \frac{1}{26}$$

一般认为，隶属度小于 0.05 时可认为不再属于所述集合，隶属度在 0.5 左右表明元素在属于与不属于所述集合之间，隶属度小于 0.5 时偏于不属于所述集合，隶属度大于 0.5 时偏于属于所述集合，隶属度大于 0.95 时基本上可认为属于所述集合。上述计算结果与我们的感觉相符合。

有了隶属度，我们还可以作模糊判断。

例如，在血液中的白细胞，正常形状是等边三角形(记为 E)。病变后的白细胞，通常呈等腰三角形(记为 I)、直角三角形(记为 R)、等腰直角三角形(记为 IR)和一般三角形(记为 T)等形状。现在有一个白细胞，我们如何判断它的形状最接近哪一种三角形？

设这个白细胞的形状为三角形 M，按大小次序依次记它的三个内角的角度分别为 A、B、C，$A \geqslant B \geqslant C$。我们分别规定 M 属于各类三角形的隶属度：

M 属于等边三角形的隶属度 μ_E 为：

$$\mu_E(M) = 1 - \frac{1}{180^\circ}(A - C)$$

我们可以检验，对任何 M，总有

$$1 \geqslant \mu_E(M) \geqslant 0$$

当 M 为等边三角形时，$\mu_E(M) = 1$。

我们规定 M 属于等腰三角形的隶属度 μ_I 为：

$$\mu_I(M) = 1 - \frac{1}{60^\circ}\min(A - B,\ B - C)$$

这里 $\min(a,\ b)$ 表示 a 和 b 中小的那个数，例如 $\min(1,\ 2) = 1$，$\min(1,\ -1) = -1$ 等等。当 M 是等腰三角形时，或有 $A = B$，或有 $B = C$，总之有 $\mu_I(M) = 1$。

M 属于直角三角形的隶属度 μ_R 为：

$$\mu_R(M) = 1 - \frac{1}{90^\circ}\ |\ 90^\circ - A\ |$$

当 M 是直角三角形时，$A = 90^\circ$，有 $\mu_R(M) = 1$。

当 M 属于等腰直角三角形的隶属度 μ_{IR} 为：

$$\mu_{IR}(M) = \min\{\mu_I(M),\ \mu_R(M)\}$$

当 M 是等腰直角三角形时，有 $A = 90^\circ$，$B = C$，有 $\mu_{IR}(M) = 1$。

M 属于一般三角形的隶属度 μ_T 为：

$$\mu_T(M) = \min\{1 - \mu_I,\ 1 - \mu_R,\ 1 - \mu_{IR},\ 1 - \mu_E\}$$

假设现在有一个三角形的三个内角依次为 85°，50°，45°，可以分别计算各隶属度为 $\mu_I = 0.916$，$\mu_{IR} = 0.916$，$\mu_R = 0.940$，$\mu_T = 0.05$，$\mu_E = 0.7$。

由于其中 μ_R 的值最大，我们判定该三角形最接近直角三角形。这种基于隶属度大小作出的判断，我们称之为模糊判断。

对于诸侯国的社会性质问题，我们可以制订一个诸侯国属于奴隶社会的隶属度指标，例如用殉葬活人数和陶俑数的比例来作为该指标。然后由考古中发现的证据，对一个春秋战国时代的诸侯国的

社会性质作出模糊判断。

对于其他类似的问题，我们也可以设计出相应的隶属度指标。当然，具体选择怎样的指标，这是各个具体学科领域内的课题。

习题

1. 有人说“我在说谎”，他是否属于所有说谎人所组成的集合？试分析说明之。

2. 把一个词分成“自适用”和“非自适用”两类。例如“汉字”两字确实是汉字，“汉字”属于自适用词；“英语”就是非自适用词。又如“古老”一词的产生确实历史悠久，“古老”属于自适用词；“摩登”也属于自适用词。试分析“非自适用”一词属于哪一类？

3. 在理发师悖论中，如果把不是理发师服务对象的人组成的集合记为 B，试分析理发师和集合 B 的关系。

4. 试寻找某种对应，以证明长度为 1 的线段和长度为 2 的线段的点集的基数相同。

5. 证明(0, 1)内的无理数集合的基数和(0, 1)内所有实数的集合的基数相同(提示：用反证法)。

6. 计算年龄为 32 岁、48 岁的人属于年轻人集合的隶属度。

7. 按课文中的判别方法，判断一个内角为 95°、35°、50°的三角形白细胞最接近文中哪一种三角形。

8. 某地区大体有四种方言。如何判断某个人使用的方言最接近何种方言？试设计一种属于某种方言的隶属度(例如用数字 1、2、…的发音)？

第二节　说变化:关系和函数

事物之间存在着各种各样的联系。例如人们之间的相互认识或血缘关系,学生成绩的优劣比较或兴趣的异同,运动队的强弱,城市之间公路连通,都是事物之间联系的例子。而事物的性质也只有从它们的相互联系中才能被认识。反映事物之间各种不同的联系,数学中也有各种关系的概念。

1. 等 价 关 系

人和人之间的血型相同、同乡、校友等关系是一种等价关系,它们具有如下的共同特性:

1) 自反性 任何一个事物总可认为自己和自己有此关系,例如自己的血型总和自己的血型相同。如果我们把 x 和 y 有相同的血型记为 $x\sim y$,则对于任何人,恒有 $x\sim x$。

2) 对称性 如果一个事物 x 与另一个事物 y 有此关系,则事物 y 与事物 x 也有此关系。例如甲和乙有相同的血型,则乙和甲也有相同的血型。用上面的记号,即为

若 $x\sim y$,则 $y\sim x$。

并不是所有的关系都有对称性。例如人们之间的认识关系就没有对称性:A 认识 B,记为 $A\sim B$,但是 B 不一定认识 A,即不一定有 $B\sim A$。

3) 传递性 如果一个事物 x 与事物 y 有此关系,事物 y 与另一个事物 z 也有此关系,则事物 x 与事物 z 也有此关系。例如甲和乙有相同的血型,乙和丙有相同的血型,则甲和丙也有相同的血型。用

上面的记号，即为

若 $x \sim y$, $y \sim z$，则 $x \sim z$。

人们的认识关系也不一定有传递性。例如 A 认识 B, B 认识 C，但 A 不一定认识 C，即此时有 $A \sim B$, $B \sim C$，但是 $A \sim C$ 不一定成立。

数学中把满足上述三个性质的关系称为等价关系。同乡、校友、相同的血型等关系都满足这些要求，都是等价关系。

在实践中，我们常常利用等价关系对所研究的事物进行分类。分类是人们认识事物性质的一种方法，而按等价关系分类恰是一种分类的抽象方法，广泛地应用于各种具体情况。这种分类方法首先要找到事物间的等价关系，再按照等价关系把事物分类，使得属于同一类的事物相互之间都是等价的，不同类的事物都没有等价关系。这样得到的每一类称为一个等价类。例如，可以证明血型相同关系是一种等价关系。按此等价关系分类，就可以把人们分为四类：A型、B型、AB型和O型。

这样的分类使人们找到了早先经常引起输血事故的原因，并采用事先验血型的方法来避免医疗事故。又如在一个地区内，如果两个城镇之间有公路连接，我们就把这两个城镇称为是连通的。可以证明，连通关系是一种等价关系。按此关系可以把整个地区划分成若干等价类：同一个等价类内的城镇可以乘汽车相互来往，不同等价类内的城镇汽车不能通行。如果设想有关部门要改善该地区的交通状况，首先可以适当地选择不同类的两个城镇，修一条公路把它们连接起来。这样原先的两个不同的等价类就变成了一个等价类，即，增加一条公路能使原先两个类内的任何两个城镇，都能够乘汽车来往。用这样的方法我们修少数几条公路就可以把该地区内的所有城镇连成一体。

2. 序 关 系

先看所有自然数所组成的集合 N：

$$\mathrm{N} = \{1, 2, 3, \cdots\}$$

两个自然数 x 和 y 之间的不等式 $x \geqslant y$ 表示了自然数 x 和 y 的大小关系，亦称序关系。这个不等式的含义是：或者 x 比 y 大，或者两者相等。序关系有下面的性质：

1) 反对称性　若有两个自然数 x 和 y 同时有不等式：$x \geqslant y$，$y \geqslant x$，则必然 $x = y$。

2) 传递性　若自然数 x、y 和 z 之间满足 $x \geqslant y$，$y \geqslant z$，则必然 $x \geqslant z$。

设想居住在某个山区的人群之间有某种血缘关系。我们现在规定，若某人 x 是另一个人 y 的长辈或与 y 同辈，我们就记为 $x \geq y$。若两个人同辈，则记为 $x = y$。在这种体系下，长辈的长辈也是长辈。这种长辈、晚辈的关系（辈分关系）也是一种序关系。可以证明这样的辈分关系"≥"满足上面的两个要求。

又如，不同血型的人之间可以输血的关系如下表：

血型		受血者			
		O	A	B	AB
输血者	O	✓	✓	✓	✓
	A		✓		✓
	B			✓	✓
	AB				✓

其中"✓"表示输血可以进行，空格表示不可进行。例如 A 型血的人可以把血输给 A 型血或 AB 型血的人，但不能输给 O 型血的人和 B 型血的人。

我们把 X 型血的人可以输给 Y 型血的人写成 $X \geq Y$。

由上面的表格我们可以验证"≥"关系满足序关系的两个要求，因而"≥"是一种序关系。

如果一个集合的序关系还满足如下的要求，则称该集合为有全序关系，称该集合为全序集。

3) 二歧性　对于集合中的任何两个事物 x 和 y，如果没有 $x \geq y$，则必有 $y \geq x$。

这个性质意味着，集合内的任意两个事物都可以按“≥”关系加以比较。没有二歧性的序关系称为偏序关系，有偏序关系的集合称为偏序集。在偏序集内的任意两个事物不一定都能比较，自然数集合按大小关系是全序集。任何两个英语单词可以按照词典序分出先后次序，这种关系满足上述三个要求，英语单词集合是一个全序集。但是上述血型的序关系不是全序关系，因为两种血型的人不一定有可输血的关系，例如 A 型血的人和 B 型血的人谁都不能把血输给对方。山区居民的辈份关系也是一种偏序关系，因为当两个人没有共同的祖先时，没有办法比较他们辈分的高低。

可以证明，在全序集内任意有限多个事物内恒有最“大”的事物。例如，在任意多个英语单词中总可以找到在词典中最早出现的一个单词；在有限多个自然数中一定可以找到一个最大的数。但是在偏序集合内，任意有限多个事物内不一定有最“大”的事物。例如，在一群山区居民中未必能找出辈分最高的人，在一群人中间也不一定有人能输血给这群人中任何一个。这个性质是全序集区别于偏序集的本质所在。

3. 相关关系和函数关系

我们先来观察现实生活中一些量的关系。例如一个人的身高与体重，一般说来，身材比较高的人身体也会比较重。又如，一个学生的数学成绩也会和他的物理成绩有一些关系，一般来说，数学成绩比较好的学生物理成绩也会比较好。有许多类似的实际例子说明有些量之间是有关系的，但是它们之间的关系和我们熟知的函数关系不同。函数关系是两个量之间确定的一种关系，当一个量（自变量）取一个值后，另一个变量（因变量）按一定的法则也随之取定一个值与之对应。例如，圆半径 R 和圆面积 S 的函数关系为

$$S = \pi R^2$$

当半径 R 确定后，圆的面积 S 按照上述公式随之确定。但是在

身高和体重的关系中，由一个人的身高并不能完全确定他的体重：不同的人身高虽然一样，体重却可以不同。这样的关系我们称之为相关关系。我们把观察到的一个量的值 x_i 和另一个量对应的值 y_i（例如一个人的身高和体重）看作一个数据对 (x_i, y_i)，并作为坐标在平面上标出相应的点，则一系列的观察数据对 $(x_i, y_i) i = 1, 2, \cdots, n$，就可以用坐标面上点的一个集合来表示。这个点的集合的图形称为相关图。在图 2.2.1 所示的六种情况下分别称两个量为强正相关，弱正相关，强负相关，弱负相关，曲线相关和不相关。

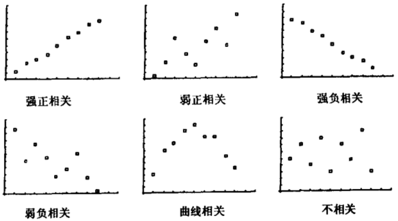


图 2.2.1

在正相关的情况下，两个量的变化方向是一致的：一个量增加，另一个量也增加；一个量减少，另一个量也减少。在负相关的情况下两个量的变化方向是相反的：一个量增加，另一个量却减少；一个量减少，另一个量却增加。正相关和负相关，通称为线性相关，因为从图上可以看出，两个量的变化和直线所表示的关系相近。在两个量为线性相关时，数学中还引进了相关系数来表明两个量关系的密切程度。相关系数 r 计算公式如下：

$$r = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \overline{y})^2}}$$

其中，$\overline{x}$是 x_1，x_2，…，x_n 的平均值：

$$\overline{x}=\frac{1}{n}\sum_{i=1}^{n}x_i$$

这里 $\sum_{i=1}^{n}x_i$ 是和式 $x_1+x_2+\cdots+x_n$ 的简写。

从理论上可以严格证明：相关系数 r 的数值范围在 -1 和 1 之间，即 $-1\leqslant r\leqslant 1$。

当 $r=1$ 或 $r=-1$ 时，x 和 y 之间就是函数关系，即由 x 的值可以完全确定 y 的值，或由 y 的值可以完全确定 x 的值。$r>0$ 时表示 x 和 y 的关系是正相关，$r<0$ 时表示 x 和 y 的关系是负相关，$r=0$ 时表示 x 和 y 之间无线性相关关系。r 的绝对值 $|r|$ 的大小表示两个量相关关系的密切程度：$|r|$ 接近 1 时表示 x 和 y 的关系是强相关，$|r|$ 接近 0 时表示 x 和 y 的关系是弱相关。一般认为，当 $|r|<0.3$ 时两个量几乎无线性相关关系，当 $|r|\geqslant 0.3$ 两个量有线性相关关系。在 0.3—0.5 之间是低度线性相关，在 0.5—0.8 之间是显著线性相关，在 0.8 以上是高度线性相关。

在实际应用时，我们可以先把两个相关量的数据对在坐标平面上描出，看看是否相关，并且在初步确定为正相关或负相关的情况下再计算两个量的相关系数，进一步从量的角度判断它们的密切程度。

例 1 某地区的气温(℃)与当天发生的交通事故数列表如下：

数据编号	1	2	3	4	5	6	7	8
气温(x℃)	14	23	16	22	30	34	19	27
交通事故数 y	4	6	3	6	8	11	5	7

我们要研究交通事故数是否和当地的气温有关。

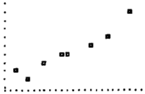


图 2.2.2

为此，我们首先把相应的数据对(14, 4)，(23, 6)，…，(27, 7)在坐标面上描出，得到表示 x 和 y 之间关系的相关图(见图2.2.2)：

从图中大体可以看出，x 和 y 之间存在正相关关系。然后计算对应的相关系数

$$r=\frac{115.75}{\sqrt{665.75}\sqrt{93}}=0.465$$

由此可知,该地气温 x 和交通事故数 y 是正相关的。

习题

1. 下列关系是否等价关系?试从等价关系必须满足的三个条件加以说明:

(1) 同乡关系; (2) 校友关系; (3) 邻居关系。

2. 验证列在孔府家谱中的人组成的集合依照辈分关系是一个全序集。

3. 在通常玩的陆军棋中规定了棋子的大小关系,这种关系是否是一种序关系?说明你的理由。

4. 足球队联赛的排名是否是一种序关系?

5. 参看下面某地区 10 个企业的数据,分析该地区企业的固定资产(百万元)和工业产值(百万元)是否相关:

(1) 画出相关图,判断是否线性相关。如果是,指出是正相关还是负相关。

(2) 计算有关的相关系数,判断相关的密切程度。看看是否和从相关图得到的结论一致。

企业编号	1	2	3	4	5	6	7	8	9	10
固定资产	3	3	5	6	6	7	8	9	9	10
工业产值	15	10	25	25	30	30	29	36	37	40

第三节　代数:运算和结构

数学研究的对象之一是结构。布尔巴基学派把数学看作是结构的学科。

1. 数学结构的概念

数学有三种母结构:代数结构,如群、环、域等;序结构,如全序、半序等;拓扑结构,如邻域、距离空间、同伦、同调等。

大多数的纯粹数学学科可以按不同的结构来加以分类。

例 1　实数系 **R** 的结构是完备的阿基米德全序域。具体地,其代数结构:域;序结构:全序;拓扑结构:$|x-y|$ 表示 x 与 y 的距离。

它还是阿基米德域,即对任何的正数 x、y,总存在一个正整数 n,使得 $n \cdot x > y$。同时,实数关于距离是完备的,即任何实柯西列都必须收敛于某个实数。

实数域与全序是协调的,因此称作为全序域,即满足

1) 加法保序性:若 $a < b$,则对任何的 c,有 $a+c < b+c$;

2) 乘正数保序性:若 $a < b$,则对任何的 $c > 0$,有 $ac > bc$。

例 2　复数系 **C** 是完备的半序域。

按照复数的加法和乘法,有

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$

$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i$$

于是复数 **C** 构成域。

它的序结构是半序,当规定 $a+bi \prec c+di$ 是指 $a \leqslant c$ 且 $b \leqslant d$。

这样规定的半序对加法是保序的，但对乘正数不保序。

例如，$0 < i$，如果两边乘以 i，但是 $0 < -1$ 并不成立。

同样规定两复数 Z_1 和 Z_2 的距离为 $|Z_1 - Z_2|$。关于这个距离复数系是完备的，即每个复数组成的柯西列必收敛于某个复数。

2. 群 的 概 念

任意两个自然数相加总是一个自然数，我们把这种性质用“在自然数集合内加法可行”来描述。同样，任意两个自然数相乘也总是自然数，因而在自然数集合内乘法也是可行的。但是两个自然数相减不一定再是自然数，我们说“在自然数集合内减法不一定可行”。同样，在自然数集合内除法也不一定可行。

由于减法和除法是加法和乘法的逆运算，我们看到，在一个集合内一种运算可行，其逆运算不一定可行。在整数集合内，加法可行，其逆运算减法也可行；乘法可行，其逆运算除法却不一定可行。等到把数的集合扩大为有理数范畴，则加法、乘法和它们的逆运算（做除法时规定除数不等于零）都可行。我们把集合和其中的运算抽象化为群的概念。

设有一个集合 G，其中的元素我们用 $a, b, \cdots$ 表示。假设在集合 G 内有一种运算，记为“$\circ$”：对 G 内的任意两个元素 x 和 y，$x \circ y$ 仍然是 G 中的元素，即在 G 中运算“$\circ$”是可行的。如果集合 G 和运算“$\circ$”还满足以下几条性质，我们就称 G 为一个群：

1) G 不是一个空集，即 G 内至少含有一个元素（事实上空集没有什么好研究的）。

2) 结合律成立：即对任何元素 a、b、c，恒有

$$a \circ (b \circ c) = (a \circ b) \circ c$$

3) 有单位元素存在，即 G 中有一个元素 e 有如下的性质：对任何 $a \in G$，恒有 $e \circ a = a$。

4) 逆运算可行，即对任何 $a \in G$，在 G 中有一个元素 a^{-1}，称为 a 的逆元，使 $a^{-1} \circ a = e$。

群的概念就是在对整数、实数等许多具体的集合和它们的运算的研究的基础上抽象出来的。在 19 世纪的最后 10 年，数学家认识到，对许多不相联系的代数系统抽出它们共同的内容进行综合的研究，可以达到事半功倍的效果。正是对群及其他一大类抽象集合和它们结构的研究，逐渐形成了近世代数这一个现代数学的分支。我们再举一些例子来说明群的概念。

例 3 整数关于加法成群。此时群的定义中的运算"∘"就是普通的加法。单位元 $e = 0$，任何一个数 a 的逆元 a^{-1} 就是 a 的相反数，即 $a^{-1} = -a$。

例 4 正有理数关于乘法成群。此时群的定义中的运算"∘"就是普通的乘法。单位元 $e = 1$，任何一个数 a 的逆元 a^{-1} 就是 a 的倒数，即 $a^{-1} = \frac{1}{a}$。

例 5 我们把在队列操练中的几个动作用记号表示出来：

保持不动记为 R_0，向右转记为 R_{90}，向左转记为 R_{-90}，向后转记为 R_{180}。记这些动作组成的集合为 M。

在 M 内规定两个动作的"∘"运算为两个动作相继进行的结果，如 $R_{90} \circ R_{-90}$ 表示先向右转再向左转，结果是保持原来的状态，即 $R_{90} \circ R_{-90}$ 等于集合中的元素 R_0。由于任意两个动作的结果总是这四个动作之一，所以 M 关于运算"∘"总是可行的。进一步，M 还关于这种运算"∘"成群：其中的单位元 $e = R_0$，各元素的逆元如下表所示。

元　素	R_0	R_{90}	R_{-90}	R_{180}
逆　元	R_0	R_{-90}	R_{90}	R_{180}

例 6 在生活中我们都知道如何计算某一天是星期几。例如某月 1 日是星期三，该月的 17 日是星期几？可以这样计算：先将 17 加 2，再除以 7 余 5，我们判断该月 17 日是星期五。

在自然数的范围内,我们把除以 7 得到相同余数的自然数归为一类。两个自然数属于同一类的特征是:它们的差可以被 7 整除。若两个自然数除以 7 以后的余数相同,我们就称这两个自然数“同余”。由有关等价关系的知识可知,同余关系是自然数集合中的等价关系。

同余关系可以把自然数分成 7 类,分别记为①、②、…、⑦。在这个集合内我们用下面的表规定类之间的加法(记为+)运算。表中数据表示 $A+B$ 的结果。可以验证这个由类组成的集合关于上面规定的加法成群。其中单位元 $e=$ ⑦。一个元素 x 的逆元就是和它相加等于 7 的那个类。例如③的逆元为④,②的逆元为⑤等等。

类中加法运算的结果

+		A						
		①	②	③	④	⑤	⑥	⑦
B	①	②	③	④	⑤	⑥	⑦	①
	②	③	④	⑤	⑥	⑦	①	②
	③	④	⑤	⑥	⑦	①	②	③
	④	⑤	⑥	⑦	①	②	③	④
	⑤	⑥	⑦	①	②	③	④	⑤
	⑥	⑦	①	②	③	④	⑤	⑥
	⑦	①	②	③	④	⑤	⑥	⑦

各类的逆元

元　素	①	②	③	④	⑤	⑥	⑦
逆　元	⑥	⑤	④	③	②	①	⑦

其实可以证明,用任何数代替 7 作为除数,可以得到相应的同余类;也用类似的方法规定类的加法运算,所得到的同余类集合也构成群,这种群称为同余类群。

例 7　我们在扑克牌的几种花色之间规定一种乘法“×”运算如

下表所示：

×	♣	♠	♦	♥
♣	♣	♠	♦	♥
♠	♠	♣	♥	♦
♦	♦	♥	♣	♠
♥	♥	♦	♠	♣

这里的第一列表示第一个因子，第一行表示第二个因子，表中的花色表示运算的结果。例如由表的第三行第四列表示以下的算式：

♠ × ♦ = ♥

事实上，如果取花色不同四张牌，则四张牌花色的乘积是♣。从其中摸一张牌，可以验证，剩下的三张牌花色的乘积恰为所缺少的花色。进一步可以验证：由此四种扑克花色组成的集合在此定义的乘法“×”下成群。扑克牌花色与这种乘法满足群的要求，单位元为♣，每种花色的逆元就是它自己。群的结构反映了扑克牌花色之间的内在关系。

例 8 由 -1 和 1 组成的集合 $M = \{-1, 1\}$ 关于乘法成群：其单位元为 $e = 1$。由 $(-1)\times(-1) = 1$，$1\times 1 = 1$，即每个元素的逆元为自己。

例 9 由“非”和“是”组成集合 $N = \{$非，是$\}$，用下列各等式规定 M 内的乘法×：

是 × 是 = 是

是 × 非 = 非

非 × 是 = 非

非 × 非 = 是

可以验证，集合 M 和关于这样规定的乘法满足所有群的要求，其单位元为 $e =$“是”。因为“非 × 非 = 是”，“是 × 是 = 是”，每个元素的逆元为自己。

如果我们把上述两例加以对比，只需把“是”看作“1”，把“非”看作“-1”，把这里规定的乘法等同于数的乘法，则两个例子中的集合 M、N 和它们的运算以及运算规律都是一样的。

例如把 N 的运算等式

$$是\times 非 = 非$$

中把“是”改作“1”，把“非”改作“-1”，就得到数的集合 M 中的运算等式：

$$1\times(-1)=-1$$

其他的等式也一样可以相互转换。

反过来，由 M 内的运算等式也可类似地转换成集合 N 中的运算等式。从这里我们还可以由数的乘法规律：奇数个 -1 之积等于 -1，偶数个 -1 之积等于 1 得到通常逻辑学中的规律：

奇数次否定之结果等于否定，偶数次否定之结果等于肯定。

上述两例说明，虽然实际背景不同，但是分别由两个元素组成的群 M、N，在某种元素和运算的对应之下，表现出相同的特性和规律。在这种情况下，我们称群 M 和群 N 具有相同的结构。

数学家研究了各种不同群的结构、表示，并进行分类。这些研究在实践中得到了多方面的应用。

3. 群的应用例子

我们讨论平面上的对称有限图形。所谓有限图形，是指整个图形可以用一个适当的正方形框起来的图形。有限图形的对称性可以用一个适当的“运动群”来刻画，这个“运动群”是由所有“经过该运动后有限图形不变”的运动组成。

对一个正方形来说，绕中心(对角线交点)顺时针旋转 90°后图形不改变，“绕中心顺时针旋转 90°”就是使正方形不变的一个运动。此外，如果将正方形绕对角线翻转，图形也不变，所以“绕对角线翻

转”也是使正方形不变的一个运动(如图 2.3.1)。绕对角线 AC 翻转后,B 点变为 D 点,D 点变为 B 点,线段 AB 变为线段 AD,线段 AD 变为线段 AB,线段 CB 变为线段 CD,线段 CD 变为线段 CB。

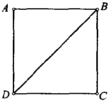


图 2.3.1

还有更多的使正方形不变的运动。如,“绕中心顺时针旋转 180°”可以看作“绕中心顺时针旋转 90°”两次,由于每次绕中心顺时针旋转 90°图形不变,因而绕心顺时针旋转 180°也使图形不变,这样,绕中心顺时针旋转 180°也是使图形不变的一个运动。一般而言,前后连续作任何两个使图形不变的运动,结果图形也不变。把两个运动按这种方式的迭加可以看作两个运动的“乘积”,经过验证可以得到,所有使正方形图形不变的运动的集合满足群的要求,这个群称为正方形的对称群。

为直观起见,我们把图形看作是一块均匀的板。使平面上任意一个有限图形不变的运动,也必然保持其重心不变。由此可以推知,这样的运动或是绕其重心的旋转,或是关于过其重心的某条直线的翻转。因而任意有限平面图形的对称群仅由绕其重心的某些旋转及关于过重心的某些直线的翻转生成。

对平面有限图形对称群的研究和分类,发现只可能出现如下几种不同情形(图 2.3.2):

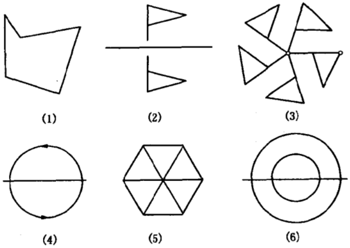


图 2.3.2

1) 仅由单位(恒等或不动)变换所组成的对称群 K_1。这是任意非对称图形的对称群。

2) 由单位变换及关于某一直线的翻折组成的对称群 K_2。

3) 只由一些旋转组成的对称群 K_3,但其中不含作任意小角度的旋转情况。

4) 只由一些旋转组成的对称群 K_4,但它含有作任意小角度的旋转。此时,作任意角度 α 的旋转仍属于群 K_4。这里的所有的运动或是图形本身或是旋转,排除了关于直线的翻转。这是平面上有方向的圆或有方向的圆环的对称群。

5) 设在平面上有 n 条过重心 O 点的直线,这些直线分平面为 $2n$ 个等角。对称群 K_5 由关于这些直线的 n 种翻转以及绕 O 旋转 $\frac{360^\circ}{2n}$ 的倍角而生成。具有这样对称群的图形包括正 $2n$ 边形。

6) 由绕 O 点所有旋转及关于所有过 O 点的直线的翻转生成的对称群 K_6。无方向圆及无方向圆环可作为它的例子。

习题

1. 举两个群的例子,说明元素是什么?运算是什么?单位元是什么?每一个元素的逆元是什么?并验证它们满足群的要求。

2. 研究下面的图形,其花纹是对哪些平面变换不变?

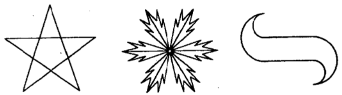


图 2.3.3

3. 对一个矩形来说,使它不变的平面变换由哪些变换组成?说明所有这些变换组成群。

4. 仔细验证例 7 中的扑克牌集合满足群的要求。试根据该例设计一个游戏:请人从一副洗好的扑克牌(除去大小王)中随便抽取

一张，不给你知道是什么牌。然后你把剩下的51张牌依次看两遍（每张牌看后须将它按原来顺序放好，切不得记录），即可猜中抽去的是什么牌。说明该游戏的原理。

第四节　几何:拓扑与图论

古老的橡皮几何游戏是让游戏者在保持曲面的光滑和完整的前提下,将其任意的变形、弯曲、伸缩和扭转,想象变形后的曲面会是什么样子?一个自行车轮胎状的环面是否会变形为一个球面?这些研究到19世纪发展成为一门新的数学分支——拓扑学。

1. 拓扑学大意

假设我们的图形是用橡皮做成的,可以使图形作各种连续变形。我们要求图形在变形的过程中保持连续而不致破裂,即原来图形上的一个点不能变成两个或两个以上的点;同时要求,图形上的点不能产生"粘合",即原来两个不同的点在变化后不能"粘合"成一个点。变形只是使图形的某些部分拉伸了,而另一些部分压缩了。

一般地说,图形在连续变形时大小、长短、形状都会改变,但是有些性质却保持不变。例如,我们可以把一根圆形的橡皮圈拉长为一个狭长的椭圆形,也可以把它变成正方形的形状,或者变成其他奇形怪状的曲线。图2.4.1画出了一些它可能变成的形状。但是圆形的橡皮圈不能变成图中的"8"字形和三叶瓣曲线。

若要变成"8"字形,必须把原先两个不同的点粘合为一个点;要变成三叶瓣曲线,必须把原先三个不同的点粘合为一个点。而这违反了"不能粘合"的变化规定。我们把所规定的变形(即可以拉伸、压缩、扭曲,不能粘合)称为"拓扑变换"(数学中的拓扑变换比这种直观的变形还要广一些)。在这种变换下不变的性质称为"拓扑性质"。图中的圆周在其变形过程中所保持的不变性质就是只有一个环,这

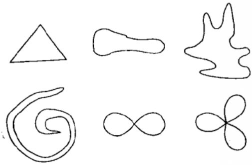


图 2.4.1

是圆周的拓扑性质。"8"字形和三叶瓣曲线分别有 2 个和 3 个环，与圆周有不同的拓扑性质。拓扑学以图形的拓扑性质作为自己的研究对象。

现在考察一个球面。我们仍然把它设想为一个可以变形的橡皮球。用拓扑变换把它变成不同的形状(图 2.4.2 是其中的一些)。

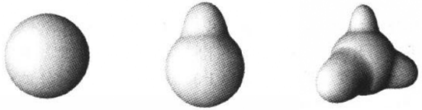


图 2.4.2

但是我们不能把它变成像救生圈那样的环面。事实上，在拓扑变换下球面有两个不变的性质，即两个拓扑性质：

1) 球面是闭曲面，它没有边界。(像救生圈那样的环面也没有边界；圆盘面是有边界的；像玻璃杯那样的曲面也是有边界的。)

2) 如果沿着球面上的任何一条闭曲线切开橡皮球，橡皮球就会分成互不联接的两部分。(像救生圈那样的环面就不具有此性质。当沿着环面的子午线切开时，环面就变成一个弯曲的圆筒形(图 2.4.3)，而这个圆筒形又可以用拓扑变换变成圆柱形的侧面。)这是球面与圆环面不同的拓扑性质。



图 2.4.3

在拓扑学中，用“连通阶”的概念来描述曲面的差别。

沿着子午线切开像救生圈那样的环面时，环面不会分开为两个互不联接的部分。这时我们说，环面上的子午线“不组成曲面的划分”。

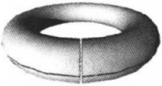


图 2.4.4(a)

在环面上，经线也不组成曲面的划分（见图 2.4.4(a)）。

在环面上可以找到两条闭曲线，一条是子午线，一条是经线，它们组合起来仍不组成曲面的划分。但是，在环面上不可能找到第三条闭曲线，使这三条曲线合起来不组成曲面的划分。这也就是说，环面上的任何三条闭曲线必定分环面为两个互不联接的部分。这时拓扑学定义环面的连通阶为 2。

对一般曲面，连通阶定义为曲面上能不组成曲面划分的最多闭曲线的数目。对球面而言，其连通阶为 0。如图 2.4.4(b)那样的面包和双柄壶，其连通阶都是 4。一般地，若在球面上开 $2p$ 个小洞，然后按两个一组配成 p 组，对每一组沿洞的边缘粘上一个圆柱面，这样得到了一个有 p 个把柄的球面。这样的曲面的连通阶是 $2p$。环面就是 $p=1$ 的情况。数学家们证明，空间的闭曲面可以按连通阶分类：任何两个相同连通阶的曲面可以从一个用拓扑变换变成另一个。

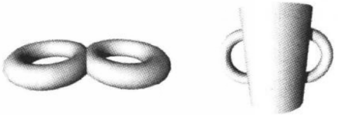
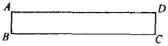


图 2.4.4(b)

但是这里仅限于双侧曲面，即它们分得出内侧与外侧。与这种曲面并存的还有所谓的单侧曲面。对单侧面来说，分不出曲面的两侧。最简单的例子是麦比乌斯带。把一个矩形的纸条 $ABCD$ 的 AB

边翻转和 CD 边粘合，使 A 和 C 粘合，B 和 D 粘合(图 2.4.5)。



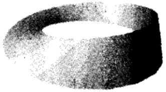


图 2.4.5

麦比乌斯带不能区分两侧。从带上一点 E 沿着带的中线移动，移动一周后回到 E 点，虽然没有经过带的边界，但是已经到了与出发时不同的一侧。此外，麦比乌斯带的边界由单独一条闭曲线组成。

麦比乌斯带是有边界的曲面，同样也存在单侧的闭曲面，即存在没有边界的单侧曲面。典型的例子是图 2.4.6 上的克莱茵曲面。设想把两条麦比乌斯带沿边界上相互粘合起来可以得到克莱茵曲面。

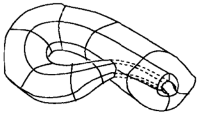


图 2.4.6

对单侧曲面也有上面所述的按连通阶分类的方法，但是各类曲面较难表现出来。

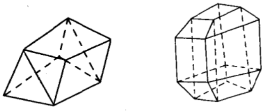
不要认为单侧曲面只是数学里的趣谈，与严肃的科学问题无关。其实早在 16—17 世纪，基于建筑、绘图、技术制图等实际应用需要而形成的理论，导致一门称为"射影几何"的数学分支产生。在一定的对应关系下可以证明，射影几何的基本对象是一个单侧的闭曲面。

2. 多面体的欧拉公式

对一个简单多面体，我们用 V 表示其顶点数，用 E 表示其棱的数目，F 表示其面的数目。数学家笛卡儿和欧拉先后独立地发现：对任何多面体，下面的公式总成立：

$$V - E + F = 2 \quad ①$$

所谓“简单多面体”，是指一个没有“洞”的多面体。如图 2.4.7(a)是简单多面体，图 2.4.7(b)不是简单多面体。



(a) (b)

图 2.4.7

上述公式①通常称为“欧拉公式”。对于我们熟悉的正多面体或是对于像图 2.4.7(a)那样的一般简单多面体，该公式都是成立的。例如对正方体，$V=8$，$E=12$，$F=6$，满足

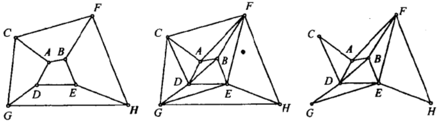
$$V-E+F=8-12+6=2$$

对图 2.4.7(a)所示的多面体，$V=8$，$E=14$，$F=8$，同样有

$$V-E+F=8-14+8=2$$

下面我们就对图 2.4.7(a)中的简单多面体来证明欧拉公式。证明的方法可以用于一般的简单多面体。这个证明富有启发性，对理解数学证明不无好处。

对图 2.4.7(a)中的简单多面体，我们设想它是空心的，且表面是由橡皮做成。我们割去多面体的一个面 $CGHF$，对剩下的表面作拉伸、压缩等连续变形(拓扑变换)，把剩下的部分展平在平面上(图 2.4.8(a))。



(a) (b) (c)

图 2.4.8

此时我们可以再进一步变形，让每一条边仍然是直线段。在这个变形的过程中，这部分的各个面的面积、棱的长度、棱与棱的夹角等等都会发生变化。但是，在平面上展平后得到的网络所包含的顶点的数目和棱的数目，仍和原来多面体的顶点数和棱数一样多。不同的是，网络所含多面体的多边形的数目，比原来多面体的面数少 1（因为展平前已经去掉了一个面 $CGHF$）。这样，我们只要证明，对于平面网络，下述公式②成立。

$$V - E + F = 1 \qquad ②$$

首先，我们把平面网络“分成三角形”：若网络的多边形不是三角形，就用添加边的方法使网络内的多边形都变成三角形（图 2.4.8(b)。注意每加一条边，同时也增加了一个面，但是顶点数不变。因此增加边的方法不会改变公式①左边 $V-E+F$（= 顶点数 − 棱数 + 面数）的数值。这说明只要讨论网络的多边形都是三角形的情况。

其次，在网络的三角形中，有些三角形的边在网络的边界上。例如图 2.4.8(b)三角形 DGC，有一条边 GC 在网络边界上。也可能网络的三角形有两条边在边界上，如图 2.4.8(c)中三角形 ADC 的 AC 和 DC 在边界上。我们取一个这样的三角形，去掉不属于其他三角形的部分。例如取图 2.4.8(b)三角形 DGC，去掉边 GC 和一个面，保留顶点 D、G、C 和边 DG 和 DC。这时，三角形 DGC 减少了一条边和一个面，$V-E+F$（= 顶点数 − 棱数 + 面数）的数值不变。而对图 2.4.8(c)中三角形 ADC，去掉边 AC、DC 一个顶点 C 和一个面 ADC，保留顶点 A、D 和边 AD。这时三角形 ADC 减少了两条边、一个面和一个顶点，$V-E+F$ 的数值仍然不变。用这种方法依次去掉边在网络边界的三角形，而每次都不会改变 $V-E+F$ 的数值。由于去掉这样的三角形后会使一些原来没有边在网络边界的三角形变成边在网络边界的情况，这个过程到有限步后得到只剩下一个三角形。而对一个三角形来说，$V-E+F$ = 顶点数 − 棱数 + 面数 $= 3-3+1=1$。由于原先的多面体比网络多一个面，因而对多面体来说，

$$V - E + F = \text{顶点数} - \text{棱数} + \text{面数}$$
$$= \text{网络的}(V - E + F) + 1 = 2$$

3. 地图的四色问题

1852 年,英国业余数学家弗朗西斯·格斯里在为英国分郡地图着色时,发现了一个看似简单但他却无法回答的问题:为任何地图着色,并使任何两个有公共边界的区域的颜色都不同,那么最少需要多少种颜色?

对于图 2.4.9 所示的包括四个国家的地图,显然需要四种颜色。但是格斯里想知道对所有的地图而言,四种颜色是否足够,是否有些地图一定要 5 种、6 种或更多的颜色?他后来又辗转向当时著名的数学家德·摩根请教。德·摩根不能回答这个问题,但是他证明了,任何地图上不会有这样的五个国家存在,其中每一个国家都和其余四个相邻。这个结论使他相信,给任何地图着色不需要五种颜色。进一步他猜想:

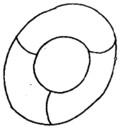


图 2.4.9

画在纸上的任何地图只用四种颜色就能使具有相同边界的国家染有不同的颜色。

这就是所谓的"四色问题"。四色问题是拓扑学中的著名问题。这里,四色问题断言,不论地图上有多少国家,也不论这些国家的位置如何,只需要四种颜色就能使相邻国家着不同色。德·摩根关于地图上不会有五个国家彼此都相邻的论据并不能作为四色猜想的证明,这里的关键问题可以用图 2.4.10 来说明:虽然图中的任何四个国家都不会和其他三个国家相邻,但是仍需要四种颜色才能使相邻国家不同色。

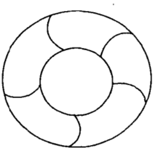


图 2.4.10

这里说的相邻国家指的是有公共的边界，而不是只有相同的一个或几个点。所谓的国家，这里假设是一个连通的区域，即区域内任何两点可以用一条完全在区域内的曲线连接起来。如果有一个国家由几个连通的区域组成，这几个区域彼此不相连通，则可以用一些具体地图说明四色猜想不成立。

1890 年达勒姆大学的数学家希伍德证明了：对任何地图，五种颜色总是足够的。但是，四种颜色同样够用在很长一段时间内仍然只是猜想。在这个猜想得到理论上的证明以前，总是存在着画出一张地图以否定四色问题的猜想的可能性。从 19 世纪中叶以来，许多著名的数学家（还有无数业余的数学家）在四色问题上倾注了大量的精力。在这个实用价值微小的问题上，数学家如此孜孜不倦地探究问题的答案，事实上与数学发展过程的一些根本问题有关。

19 世纪末，数学家建立了许多强有力的理论，使他们能解决许多困难的问题。这些成功使他们觉得，只要是用数学语言合理地提出的问题，总是能够用适当的理论来解决的。对于四色问题，很容易用数学语言使任何外行人一听就懂。数学家之所以没有解决这个问题，是因为数学家还没有发现适当的数学方法。

但是这个信念在 20 世纪中叶受到了冲击。30 年代的奥地利数学家哥德尔在有关数理逻辑的研究中发现，在似乎最自然的逻辑系统中，有些语句是真的，但不能在这个体系里得到证明。还有一些可以用很简短的语句陈述的语句，但其最短的证明也会是非常长，以至于不可能在合理的时间内写下来。在 50 年代，数学家发现，同样的困难在数理逻辑以外的数学分支也存在。于是有些人认为，既然四色问题的猜想研究了这么长的时间都没有解决，它可能也是既不能否定也无法肯定的问题。也有些人认为，这个猜想是对的，但是问题的证明本质上长得无法写下来。还有一些人认为，上述的危机还不至于发生在四色问题上，必定有一个巧妙的数学推理最终证明或否定这个猜想。

经过许多数学家的努力，把四色问题归结为近二千种情况的证明。但是靠人工一个一个地完成判断和证明是不可能的。终于在

1976年,三位美国科学家阿沛、哈肯和摩尔借助于当时先进的计算机,花了1 200小时,作了近100亿个逻辑判断,才最终证明了四色问题。至于这样的证明算不算证明,则是个哲学问题了。

四色问题,讨论的是球面上或平面上的地图着色。而在另外类型的曲面上,情况就不是这样。例如,对像救生圈一样的圆环曲面,早在四色问题得到证明以前有人就已经证明了,用七种颜色就可以给这种曲面上的任何地图着色,而且实际画出了一张有七个国家的地图,该地图上的每一个国家都和其余六个国家相邻。这个"奇异"的性质说明了球面和环面根本的差异。

习题

1. 试做一个麦比乌斯带,验证它是一个单侧曲面,验证其边界是一条闭曲线。再沿着麦比乌斯带的中线剪开,剪以前想一下会得到什么样子的曲面,与实验得到的结果比较。

2. 对图5中的曲面,试画出不组成曲面划分的闭曲线,分别看看最多有几条这样的曲线。

3. 下面的曲面哪些在拓扑变换下是相同的?

脸盆,草帽,鞋子,围巾,汗衫,无镜片的眼镜,运动裤,袜子,搭扣皮带(使用时和不使用时)。

4. 对连通阶为0、2、4、6的情况各举一个实用物品的例子。

5. 对下列图形验证欧拉公式:

四面体,五棱柱,长方体。

6. 如果一个正多面体的每个面是等边三角形,并且各个顶点所在的三角形都一样多,这样的多面体的面有几种?

7. 一个足球由32个正五边形和正六边形缝制而成。问五边形和六边形各有几个?

第五节　矩阵:生活中的数学

在今天这个数字化时代,对公民来说,最重要的知识和技能是什么?美国芝加哥大学的 Z·尤什斯金教授认为,数据处理是最基本的内容之一,它甚至比解方程和几何证明更基本。为此我们在这里利用大家在生活中熟悉的实例,介绍一些最基本的数据处理方法。

1. 超市里的向量和矩阵

当我们在超市里消费的时候会发现,那里收银员的记账、算账方式比传统的营业员简单、利索、准确得多,这一切归功于超市的计算机管理系统和科学的数学工具。

(1) 向量

在物理课中学过向量,即具有大小和方向的量称为向量。例如,力,有大小和方向,因而是向量。然而,超市怎么会和向量有关呢?

在中学教材的复数这一节里,说过复数 z、平面向量$\overrightarrow{Oz}$和一对实数(a, b)是一一对应的:

$$z = a + bi \leftrightarrow (a, b) \leftrightarrow \overrightarrow{Oz}$$

请大家注意,(a, b)无非是两个有序的实数。推而广之,我们把 n 个有序的数据 $a_1, a_2, \cdots, a_n$ 称做一个 n 维向量 A,它有 n 个坐标,记作:

$$A = (a_1, a_2, \cdots, a_n)$$

这样的 n 维向量,我们随处可见,并不陌生。看看你每个月的工资单:

职务工资	岗位津贴	书报费	午餐补贴	奖金	总数
800	230	40	100	350	1 520

这就是一个 6 维向量。所谓"有序",是指每个位置都有特殊的意义,不可随意颠倒。

向量的好处是表述简单,运算简便。例如它们可以作加减运算,即把它们的对应项相加(减)法就是了:

若 $A=(a_1, a_2, \cdots, a_n)$, $B=(b_1, b_2, \cdots, b_n)$,

则 $A+B=(a_1, a_2, \cdots, a_n)+(b_1, b_2, \cdots, b_n)$

$=(a_1+b_1, a_2+b_2, \cdots, a_n+b_n)$。

如果你要计算两个月工资收入的分类明细数目,只需要把两个月的工资向量相加:

$$A=(800, 230, 40, 100, 350, 1\,520)$$

$$B=(800, 160, 40, 0, 0, 1\,000)$$

则 $$A+B=(1\,600, 390, 80, 100, 350, 2\,520)$$

一个企业的财务科,需要把每个员工的"工资向量"保存在计算机里,于是要统计全体员工的工资总额、奖金总额、书报费总额等等,只需将各人的工资向量统统加起来,就一清二楚了。

向量不仅可以相加,还可以相乘。现在让我们来看一个超市里买东西的情形。

超市里有很多种商品,为了简单起见,不妨假设只有 5 种:蛋、糖、奶粉、藕粉和香肠。我们将它们编上号码,依次为 1 号、2 号、3 号、4 号和 5 号。于是每一笔生意都与 5 维的顾客购货量向量

$$A=(a_1, a_2, \cdots, a_5)$$

和 5 维的价格向量

$$B=(b_1, b_2, \cdots, b_5)$$

有关,其中 a_i 表示顾客购买第 i 号货物的数量,b_i 表示第 i 号货物的单价 $(i=1, 2, 3, 4, 5)$。

如果一位顾客买了4斤蛋、1斤糖和10斤藕粉。于是我们便得到这位顾客的购货向量：

$$A=(4,1,0,10,0)$$

假设上述5种商品的单价为：

	蛋 (500克)	糖 (500克)	奶粉 (500克)	藕粉 (500克)	香肠 (500克)
单价(元)	1	0.7	3	0.2	4

于是我们有价格向量

$$B=(1,0.7,3,0.2,4)$$

那么顾客应付款应该是

$$\begin{aligned}&4\times1+1\times0.7+0\times3+10\times0.2+0\times4\\=&4+0.7+2=6.70(\text{元})\end{aligned}$$

我们把6.70叫作购货向量 A 和价格向量 B 的数量积，记作

$$A\cdot B=(4,1,0,10,0)\cdot(1,0.7,3,0.2,4)$$

对这个超市来说，每一笔生意只需用一个5维向量

$$A=(a_1,a_2,\cdots,a_5)$$

就能记录下全部购货信息。对于超市来说，商品的价格、店中货物的库存量、每日销售总量也都是向量。因此管理一个商店，所接触的数字信息可以说都是向量，所进行的统计运算都是向量的加减和数量积。大型超市有成千种商品，成万笔生意，就需要考虑成万个成千维的向量，人工记录和计算工作量很大，也容易出错，于是就把这些机械的记忆和计算规则由计算机去执行，这就是计算机管理。其实这里用到的最基本的数学工具就是向量的运算！主要涉及向量的加减和数量积，这两种运算的一般法则是：

$$\begin{aligned}A\pm B&=(a_1,a_2,\cdots,a_n)\pm(b_1,b_2,\cdots,b_n)\\&=(a_1\pm b_1,a_2\pm b_2,\cdots,a_n\pm b_n)\end{aligned}$$

$$A \cdot B = (a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n)$$
$$= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

从上面的例题和法则可见，两个同样维数的向量才能进行加减和数量积运算；两个向量加减的结果是一个向量，两个向量的数量积是一个数。

(2) 矩阵

超市里一般有很多顾客，要记录、管理和计算很多向量，这时也可把矩阵作为工具。

例如，有 A_1、A_2、A_3、A_4 四个顾客，他们购货数量如下：

	蛋 (500 克)	糖 (500 克)	奶粉 (500 克)	藕粉 (500 克)	香肠 (500 克)
A_1	4	1	0	4	0
A_2	7	10	5	0	0
A_3	10	8	7.5	100	31
A_4	2.5	7	6.4	232	9

我们把表中的数构成有序(在横向和纵向两个方向上都有序)的“数字阵”

$$A = \begin{bmatrix} 4 & 1 & 0 & 4 & 0 \\ 7 & 10 & 5 & 0 & 0 \\ 10 & 8 & 7.5 & 100 & 31 \\ 2.5 & 7 & 6.4 & 232 & 9 \end{bmatrix}$$

叫做购货的数量矩阵。这是一个四行五列，即 4×5 的矩阵。每一行都是一个 5 维的向量，它们分别表示四个顾客购货的数量矩阵，它们与单价矩阵的数量积分别表示四个顾客应付的款数，这四个数量积构成的向量：

$$\begin{bmatrix} 4 & 1 & 0 & 4 & 0 \\ 7 & 10 & 5 & 0 & 0 \\ 10 & 8 & 7.5 & 100 & 31 \\ 2.5 & 7 & 6.4 & 232 & 9 \end{bmatrix} \begin{bmatrix} 1 \\ 0.7 \\ 3 \\ 0.2 \\ 4 \end{bmatrix} = \begin{bmatrix} 5.5 \\ 29.0 \\ 182.1 \\ 109.0 \end{bmatrix} \quad ①$$

就是矩阵 A 与向量 B 的乘积，记作 $A \cdot B$。

从计算中我们不难看出，在进行矩阵与向量的乘法时，矩阵的列数必须与向量的维数相同，而积向量的维数恰与矩阵的行数相同。

在①式中，我们把价格向量写成有序的一列数，它的实际意义与写成一行数是一样的，只是满足数学表达上的规范性要求而已。写成 $(a_1, a_2, \cdots, a_n)$ 的 n 元向量可看作是 $1 \times n$ 的矩阵；写成

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$$

的 n 元向量可看作是 $n \times 1$ 的矩阵。因此①式也可看作是矩阵与矩阵的乘法。

作为经营单位，超市是需要计算利润的。如果上述五种商品的单位利润如下：

	蛋（500 克）	糖（500 克）	奶粉（500 克）	藕粉（500 克）	香肠（500 克）
利润（元）	0.2	0.1	0.3	0.05	0.4

利润额的计算方法与营业额的计算方法一样，只要求出顾客购货的数量矩阵 A 与单位利润向量 $C = (0.2, 0.1, 0.3, 0.05, 0.4)$ 的乘积：

$$A \cdot C = \begin{bmatrix} 4 & 1 & 0 & 4 & 0 \\ 7 & 10 & 5 & 0 & 0 \\ 10 & 8 & 7.5 & 100 & 31 \\ 2.5 & 7 & 6.4 & 232 & 9 \end{bmatrix} \begin{bmatrix} 0.2 \\ 0.1 \\ 0.3 \\ 0.05 \\ 0.4 \end{bmatrix} = \begin{bmatrix} 1.1 \\ 3.9 \\ 22.45 \\ 18.32 \end{bmatrix} \qquad ②$$

②式右边就是每笔生意的利润额。

如果超市要在计算每笔生意的营业额同时，可一并计算其利润额，那么就应该进行如下的矩阵乘法：

$$
\begin{bmatrix} 4 & 1 & 0 & 4 & 0 \\ 7 & 10 & 5 & 0 & 0 \\ 10 & 8 & 7.5 & 100 & 31 \\ 2.5 & 7 & 6.4 & 232 & 9 \end{bmatrix} \begin{bmatrix} 1 & 0.2 \\ 0.7 & 0.1 \\ 3 & 0.3 \\ 0.2 & 0.05 \\ 4 & 0.4 \end{bmatrix} = \begin{bmatrix} 5.5 & 1.1 \\ 29.0 & 3.9 \\ 182.1 & 22.45 \\ 109.0 & 18.32 \end{bmatrix} \quad ③
$$

仔细观察,可见③式的左边的第一个矩阵是购货的数量矩阵,第二个矩阵是单价向量和利润向量构成的矩阵,它们的乘积得到右边的矩阵,这个矩阵的第一列是每笔生意的营业额,第二列是每笔生意的利润额。这就是矩阵与矩阵的乘积。同理,如果该超市还要计算每笔生意所产生的其他指标额(如成本、损耗等等),也可类似地同时进行。

一般地,两个矩阵的乘积的运算方法如下:

$$
设\ A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},\ B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1l} \\ b_{21} & b_{22} & \cdots & b_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nl} \end{bmatrix}
$$

则矩阵 A 与 B 的乘积 AB 等于矩阵

$$
C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1l} \\ c_{21} & c_{22} & \cdots & c_{2l} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{ml} \end{bmatrix}
$$

其中

$$
c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}
$$

$$
i = 1,\ 2,\ \cdots,\ m \quad j = 1,\ 2,\ \cdots,\ l
$$

向量和矩阵在实际生活和理论研究中都有非常广泛的应用,上述仅是最简单的一例。

2. 体育比赛中的评分规则

大千世界,到处是数据:每个人的身高和体重、每个学生的成绩、每个工人的工资、每个灯泡的寿命、每场比赛的得分等等,一大堆的原始数据往往会使人眼花缭乱,难以把握。如果能用一个代表数,来概括地、准确地刻画这一大堆数据的特征,将是十分必要的。例如,我们常说:"我班的数学成绩平均为 82 分";"某公司职工的平均工资为 2 200 元";"某种品牌的灯泡的平均寿命为 1 000 小时";"一场篮球赛中,平均每个队员的得分数为 25 分"等等。这些都是用一个代表数来刻画许多数的例子。

那么对于 n 个数 $x_1, x_2, \cdots, x_n$,怎样来选取代表数呢?

最常用的代表数是用算术平均数

$$\bar{x} = \frac{1}{n}(x_1 + x_2 + \cdots + x_n)$$

作为代表数。上面的例子中的代表数几乎都是算术平均数。

另一种常用的代表数是中位数。中位数的一般定义如下:

设有 n 个数据,将他们从小到大依次排列为

$$x_1,\ x_2 \cdots\ x_n$$

如果 n 是奇数时,那么第 $\frac{n+1}{2}$ 项的值就是该组数据的中位数;如果 n 是偶数时,那么第$\frac{n}{2}$项和第 $\frac{n}{2}+1$ 项的平均值就是该组数据的中位数。

例如数据组

6, 6.5, 6.6, 6.6, 6.65, 6.7, 6.8, 6.8, 8,

它的中位数为 6.65。如果再添上一个数据 9,则数据组的中位数为

$$\frac{6.65 + 6.7}{2} = 6.675$$

平均数和中位数对原始数据组都有比较好的代表性，其中平均数能概括地表现所有数据的集中态势，而中位数准确地表示出数据的中等水平。但它们也各有局限性，例如个别特别大或特别小的孤立数据，极有可能是不正常数据，但它却能影响平均数的大小；而对于中位数来讲，事实上影响中位数大小的只是原始数据组中极少量的几个数据，其他大部分数据的大小没有充分体现出来。

因此在竞争剧烈的体育比赛中，为了评分的公平，常常先由几个裁判分别评分，然后将裁判的评分"去掉一个最高分，去掉一个最低分"，求其他分数的平均值作为运动员的得分。这样的评分规则有什么好处呢？我们具体地分析一下。

设有五个裁判对一位运动员的表现进行评判，它们的评分依次为

$$8.6,\ 8.8,\ 9,\ 9.3,\ 9.3$$

这里平均数和中位数都是9。

如果某个裁判出于偏见，故意压低该运动员的得分，例如现在的评分为

$$8.1,\ 8.8,\ 9,\ 9.3,\ 9.3$$

这时的平均分为8.9分，而中位数仍然是9分。可见，个别裁判的不公正评分(过低或过高)会影响平均分，但一般不影响中位数。

由于评分总有随机性，即使裁判对运动员没有偏见，不会故意压低或提高分数，随机误差也是不可避免的。如果一位裁判把原9分打成9.2分，于是评分结果为

$$8.6,\ 8.8,\ 9.2,\ 9.3,\ 9.3$$

这时平均分为9.04分，而中位数为9.2分，比平均数的改变大得多。这是因为中位数仅仅依赖于处在最中间的一个或几个数据，几乎完全不反映两旁的数据变化，使得处在中间的数据误差被不合理地扩大为整体数据的误差，而平均数的算法却能将这类误差合理地分解了。

因此,采用"去掉一个最高分,去掉一个最低分",求其他分数的平均值的规则既可以降低极端分数的影响,又可以避免给中间几个数据太大的权重,合理地分解所有裁判的评分误差。

除了平均数和中位数之外,众数也可作为数据组的代表数,即数据组中重复出现次数最多的那个数据。在上述数据组中,9.3 就是众数。

3. 有奖销售与彩票

美好的愿望总是与风险并存。人们在投资时总是希望有高的回报率,但有时会血本无归;人们在买彩票时总是希望能中奖,但往往会一次又一次的失望,这是大多数人在生活中经历过的体会。尽管如此,但人们还是一次又一次满怀希望地冒险,然后尝试成功的喜悦或失败的懊恼。一般来说,我们无法确定自己美好的愿望是否会圆满地实现,但是我们应该估计到自己冒的风险有多大。数学家以期望值来分析风险,衡量风险的大小,以便作出正确的决策。

帕斯卡(Pascal)首先提出了数学期望值的概念:如果卖出彩票1 000张,奖金总额为 500 元,那么你每购买一张彩票的期望值为

$$500 \times \frac{1}{1\,000} = 0.50(\text{元})$$

如果你买了 600 张,那么期望值将是

$$0.5 \times 600 = \frac{600}{1\,000} \times 500 = 300(\text{元})$$

一般地,定义期望值 E 为概率 p 乘以奖金数 A:

$$E = pA$$

为了便于解释期望值的计算公式,我们假设在每 1 000 张彩票中,有 2 张中奖 100 元,有 1 张中奖 300 元。如果你只买 1 张彩票,那么可能获奖金 300 元,也可能获奖金 100 元或者没有奖金,究竟会

出现哪种情况是无可预料的。但是如果你买彩票较多的话，那么根据彩票总体的情况，你每买 1 000 张彩票，平均可能会出现 997 张空票（没有奖金）、2 张 100 元、一张 300 元的情况。所以每当你买了 1 000张彩票时，可计算得的奖金额平均应该是

$$997 \times 0 + 2 \times 100 + 1 \times 300 = 500(\text{元})$$

于是你只买 1 张彩票时，平均的奖金额应该为

$$\begin{aligned}&\frac{997 \times 0 + 2 \times 100 + 1 \times 300}{1\,000}\\ &= \frac{997}{1\,000} \times 0 + \frac{2}{1\,000} \times 100 + \frac{1}{1\,000} \times 300\\ &= 0.997 \times 0 + 0.002 \times 100 + 0.001 \times 300\\ &= 0.5(\text{元})\end{aligned}$$

上述结果可以表达成公式，即数学期望

$$E = p_1 \cdot A_1 + p_2 \cdot A_2 + p_3 \cdot A_3\text{。}$$

其中 A_1，A_2，A_3 是各种不同的奖金额，p_1、p_2、p_3 分别是获得奖金 A_1，A_2，A_3 的概率。

更一般地，如果一个随机变量 x（上述问题中是所获奖金额）所有可能出现的状态有 A_1，$A_2 \cdots A_n$，而出现这些状态的概率依次是 p_1，$p_2 \cdots p_n(p_1 + p_2 + \cdots + p_n = 1)$，那么随机变量 x 的期望值

$$E = p_1 \cdot A_1 + p_2 \cdot A_2 + \cdots + p_n \cdot A_n$$

事实上，数学期望就是算术平均数的推广。

例 1　有一场赌博的规则如下：掷一个正六面体骰子，若出现 1，则你赢 10 元；若出现 2、3 或 4，则你输 2 元；若出现 5 或 6，不输不赢。问这样的规则对你是否有利？

对于这样的问题，我们应该计算期望值。出现 1 的概率是 $\frac{1}{6}$，出现 2，3 或 4 的概率是

$$\frac{1}{6}+\frac{1}{6}+\frac{1}{6}=\frac{1}{2}$$

出现 5 或 6 的概率是 $\frac{1}{6}+\frac{1}{6}=\frac{1}{3}$，所以期望值

$$E=\frac{1}{6}\times 10+\frac{1}{2}\times(-2)+\frac{1}{3}\times 0=\frac{2}{3}$$

因此，这场竞赛对你是有利的。

以上我们举的是掷骰子、买彩票的例子，但并不是只有赌博才会碰到期望值问题。事实上我们天天在和期望值打交道。

例 2 一家个体户有一笔资金，如果经营西瓜，风险大但利润高（能赚的概率为 0.7，获利 2 000 元）；如经营工艺品，风险小但获利也小（能赚的概率为 0.95，利润为 1 000 元）。究竟该如何决策？

若经营西瓜，则期望值 $E_1=0.7\times 2000$，即 1 400 元；而经营工艺品，期望值 $E_2=0.95\times 1000$，即 950 元。所以权衡下来，情愿“搏一记”，去经营西瓜，因它的期望值较高。

期望值这个概念，并不是很容易接受的。在有些人看来，如果中奖就拿 500 元，不中奖就一分钱也没有，这个期望值 0.5 元（中奖概率 0.001 乘以 500）是个什么“东西”？应该说我国公民对这一数学知识的理解和认识还是很差的，远不及“平均数”和“百分比”那样普及。但是在商品经济不断发展的今天，风险处处存在，决策时时要作。如无“期望值”的概念，作为领导者也许会对专业人员写的可行性报告也看不懂，那怎么进行工作？

这里我们不妨举一个某省关于某工程的投资决策的实例。

例 3 某新工艺流程如投产成功可收益 300 万元。但投产之前，必须经过小型试验和中型试验，试验经费分别需 2 万元和 36 万元。小型试验的成功率为 0.7，如果连做两次小型试验，则成功率可提高到 0.8，在小型试验基础上的中型试验的成功率为 0.7，如果直接搞中型试验的成功率为 0.5。应该如何决策，才能获利最多？

解　共有三种决策：

① 一次小型试验和一次中型试验。此时工程的所有可能情况及其概率如下：

方案	小型试验		中型试验		累计概率	试验花费	实际收益
	成败	概率	成败	概率			
①	成功	0.7	成功	0.7	0.49	38	262
			失败	0.3	0.21	38	−38
	失败	0.3			0.3	2	−2

工程投资获益的期望值

$$E_1 = 0.49 \times 262 + 0.21 \times (-38) + 0.3 \times (-2) = 119.8(\text{万元})$$

② 两次小型试验和一次中型试验，此时工程的所有可能情况及其概率如下：

方案	两次小型试验		中型试验		累计概率	试验花费	实际收益
	成败	概率	成败	概率			
②	成功	0.8	成功	0.7	0.56	40	260
			失败	0.3	0.24	40	−40
	失败	0.2			0.2	4	−4

工程投资获益的期望值

$$E_2 = 0.56 \times 260 + 0.24 \times (-40) + 0.2 \times (-4) = 135.2(\text{万元})$$

③ 有些领导急于求成，想省去小试，直接搞中试，此时工程的所有可能情况及其概率如下：

方　案	中型试验		试验花费	实际收益
	成败	概率		
③	成功	0.5	36	264
	失败	0.5	36	−36

工程投资获益的期望值

$$E_3 = 0.5 \times 264 + 0.5 \times (-36) = 114(\text{万元})$$

显然，这时采取第二方案最有利。试想，如果一位领导者没有概率知识，对期望值概念一无所知，那么他如何做出科学的决策呢？

不但企业的领导人需要决策，一般的公民和消费者也要学会用期望值进行决策。

例 4 某人有 10 万元，有两种投资方案：一是购买股票，二是存入银行获取利息。买股票的收益取决于经济形势，假设可分三种状态：形势好、形势中等、形势不好(即经济衰退)。若形势好可获利 40 000 元，若形势中等可获利 10 000 元，若形势不好要损失 20 000 元。如果是存入银行，假设年利率为 8%，即可得利息 8 000 元。又设经济形势好、中、差的概率分别为 30%、50% 和 20%。试问应选择哪一种方案可使投资的效益更大？

下面给出采用期望值作为标准的解法。

设 a_1 为购买股票，a_2 为存银行，θ_1 为经济形势好，θ_2 为经济形势中等，θ_3 为经济衰退，$P(\theta_i)(i = 1, 2, 3)$ 为三种形势的概率，a_{ij} 为第 i 种方案和第 j 种状态结合的结果，把它们列成一张表(称之为报偿表)，即：

	θ_1	θ_2	θ_3
	$P(\theta_1) = 0.3$	$P(\theta_2) = 0.5$	$P(\theta_3) = 0.2$
a_1	$a_{11} = 40\ 000$	$a_{12} = 10\ 000$	$a_{13} = -20\ 000$
a_2	$a_{21} = 8\ 000$	$a_{22} = 8\ 000$	$a_{23} = 8\ 000$

从上表可以看出，如果在经济形势好(θ_1)和经济形势中等(θ_2)的情况下，那么购买股票是合算的；但如果经济形势衰退(θ_3)，那么采取存银行的方案比较好。然而人们事先是不知道哪种情况会出现，因此采用期望值标准是比较合理的。方案 a_1，a_2 的期望值分别为：$E_1 = 40\ 000 \times 0.3 + 10\ 000 \times 0.5 + (-20\ 000) \times 0.2 = 13\ 000(\text{元})$，$E_2 = 8\ 000(\text{元})$。

因为 $E_1 > E_2$，所以方案 a_1 期望的收益比 a_2 大。按最大收益原则，应采用期望收益高的方案，淘汰期望收益低的方案，所以应采用购买股票的方案。

第六节　统计:聚类与层次分析

分类是人类认识客观世界的基本方法之一。人们把所研究的对象分成若干类,然后分门别类地进行仔细研究,从而加深对事物的认识。例如通过对感冒病人病史的分类,会加深对感冒病因的认识;对公司经营业绩分类,可以找到改善经营的途径。历史上很早以前就有分类学这门学问,但那时主要靠专业知识进行分类,很少利用数学工具。随着生产和科学技术的发展,分类越来越细,对分类准确性的要求越来越高,于是分类学中逐渐应用数学方法,逐渐形成了“聚类分析”或“聚类建模”的学问。

有许多方法来衡量两个事物的接近程度。我们将每个事物看作数学空间中的一个点,在这个数学空间中规定了两点间的距离,以距离来表示事物的差别程度,分类时把距离近的点归成一类。这就是最基本的聚类思想。

1. 有序事物的聚类分析

例 1　儿童每年增加的重量与儿童的生长发育过程有关。下表列出 1 至 11 岁儿童每年平均的增重数:

年　龄	1	2	3	4	5	6	7	8	9	10	11
增重(千克)	9.3	1.8	1.9	1.7	1.5	1.3	1.4	2.0	1.9	2.3	2.1

从表中可以粗略地看到:1 岁是儿童增重的高峰;6 岁是儿童增重的低谷。我们来讨论:应该把 1 岁至 11 岁的儿童分成几个发育阶段?如何划分阶段为好?

许多实际问题中的事物是按一定次序排列的，这样的事物称为有序事物。如例题中儿童的增重数按年龄排序；历史的研究按时间的先后排序；地质勘探取样资料按地层的深浅排序等。对有序事物分类时不能打乱原先事物的次序。我们现在就以上述儿童增重的问题为例，介绍有序事物分类的方法。

以 $x_1, x_2 \cdots x_{11}$ 记与年龄对应的儿童增重数的 11 个数据，x_i 表示 i 岁儿童的增重数，例如 $x_8 = 2.0$ 表示 8 岁儿童的平均年增重为 2.0(千克)。如果要把增重数 $x_1, x_2, \cdots, x_{11}$ 分成保持次序的 3 个组，这时可以有多种的选择。例如

$$\{1, 2, 3\}, \{4, 5, 6, 7, 8\}, \{9, 10, 11\}$$

就是一种可选择的分类方法。这里 $\{1, 2, 3\}$ 表示把 1—3 岁分为一组，$\{4, 5, 6, 7, 8\}$ 表示把 4—8 岁分为一组等等。可以理解：把 11 个事物不改变其排列次序地分为 3 类，相当于在 10 个位置(每个位置想象为两个事物之间的“间隔”)放置 2 个栅栏。因此按组合方法总共有 $C_{10}^2 = 45$ (组合数)种分法。

一种好的分类方法，应该使处于同一类事物之间的差别尽可能地小，而使类与类之间的差别尽可能地大。例如我们把一个班级的学生分成学习成绩好、中、差三类，同是成绩好的一类的学生之间应该差别不大，而若一个属于成绩好的一类，另一个属于成绩中的一类，则这两个学生就应有明显的差别。为了表示类内部事物与事物的差别，我们借用统计中全距的计算方法。

现在我们以下面的一种分类方法：

$$\{1, 2, 3\}, \{4, 5, 6, 7, 8\}, \{9, 10, 11\}$$

为例，说明计算类内差别的方法。其中第一类 $\{1, 2, 3\}$ 对应的数据为：9.3，1.8，1.9。此处最大值为 9.3，最小值为 1.8，这一类内的差异我们用其全距

$$9.3 - 1.8 = 7.5$$

来表示。第二类 $\{4, 5, 6, 7, 8\}$ 对应的数据中最大值和最小值分别

为:2.0, 1.3,于是这一类内的差异用

$$2.0-1.3=0.7$$

来表示。同理,第三类{9, 10, 11}的类内差异用

$$2.3-1.9=0.4$$

表示。为衡量上述分类方法的优劣,我们计算此种分类方法中的三个类内的平均差异,即规定该分类方法的优劣指标 K 为

$$K=\frac{7.5+0.7+0.4}{3}=2.87$$

对于另一种分类方法

$$\{1, 2, 3, 4\}, \{5, 6\}, \{7, 8, 9, 10, 11\}$$

其第一类的类内差异为 7.6,第二类的类内差异为 0.2,第三类的类内差异为 0.9。该分类方法的优劣指标为 2.9。相比之下,此分类方法不如前一种分类方法好。把 11 个有序数据分成 3 类共有 45 种方法,计算每种分法的优劣指标并加以比较,可以得到最好的(分三类)方法为

$$\{1\}, \{2, 3, 4, 5, 6, 7\}, \{8, 9, 10, 11\}$$

此分类方法的优劣指标 K 是 0.30。

以同样的方法分析,可知把这 11 个数据分成两类的最好分类方法是

$$\{1\}, \{2, 3, \cdots, 10, 11\}$$

这时的优劣指标 K 为 0.5。那么这 11 个数据分成几类为宜呢?

为此,我们分别找到把 11 个数据分成 1 类、2 类、…、11 类的最好的分类法,计算出各最好分类方法的优劣指标,列表如下:

n	1	2	3	4	5	6	7	8	9	10	11
K	8.0	0.5	0.3	0.2	0.14	0.1	0.07	0.04	0.02	0.01	0

由表可看到，如果把 1 至 11 岁的数据只分成一类 ($n = 1$) 时，$K = 8$，优劣指标值太大；而对 n 大于 4 时的 K 值相差不多；而当 $n = 3$ 或 $n = 4$ 时，K 值已降为 0.30 和 0.20。因此分成 3 类或 4 类为宜。

我们也许可以对分成三类的情况予以如下实际解释：

儿童从 1 岁到 11 岁可分为三个阶段：1 岁的儿童睡得多吃得多，处于体重增加最快的阶段；2 岁至 7 岁的儿童处于入学前或刚入学的阶段，体重增加有所减缓；8 岁至 11 岁后生活规律化，开始进入发育期，体重稳定增加。

2. 系 统 聚 类

在各种分类方法中，系统聚类是被应用最广泛的方法之一，它的聚类步骤简述如下：

假设要将 n 个事物分类。

1) 先将 n 个事物各自看成一类，这样开始时共有 n 类；

2) 规定事物之间的距离 d，以表示事物之间差别；同时规定类与类之间的距离 D，以表示类之间的差别。开始时，由于 n 个事物各自成一类，故类与类之间的距离就是事物间的距离；

3) 将距离最小的两个类合并成一个新类，计算新类与其他类的距离，再将距离最近的两类合并。

每次合并可减少类的数目，直至类的数目满足聚类的要求为止。这种方法称为系统聚类。

现在以 $d(i, k)$表示第 i 个事物与第 k 个事物间的距离。类与类的距离可以用如下的方法规定：

设 G_1，G_2，…表示类，用 $D(p, q)$记类 G_p 与类 G_q 之间的距离。类间距离有多种定义方法，常用的有最短距离、重心距离、闵考夫斯基距离等等，我们在下面的例题中，不妨把 $D(p, q)$规定为 G_p 和 G_q 之间的“最短距离”，即 G_p 中任一事物与 G_q 任一事物距离的最小值。

例　对某地 21 个古墓挖掘后，记录每个古墓陪葬的瓷器用具数和陶俑数，分别记为 x_1 和 x_2。要求按这两个指标对古墓进行分类。数据列表如下：

古墓文物数据

古墓号	1	2	3	4	5	6	7	8	9	10	11
x_1	5	5	7	7	9	9	10	11	11	12	8
x_2	11	10	10	8	9	8	6	7	6	5	9
古墓号	12	13	14	15	16	17	18	19	20	21	
x_1	3	2	2	0	6	5	5	4	4	2	
x_2	7	7	5	7	6	4	3	4	2	0	

此处，x_1 和 x_2 可以看作平面直角坐标系中点的两个坐标，每个古墓可以用该坐标平面上的一个点来表示，得图 2.6.1。我们采用通常平面上点的距离作为对应的古墓与古墓间的差别。

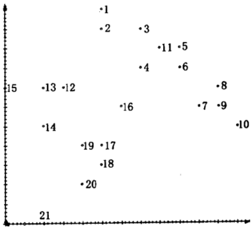


图 2.6.1

第一，从图和表都可看出，两个古墓的最小距离是 1，其中下面几组古墓之间的距离都是 1：

1 号与 2 号，5 号与 6 号，11 号与 5 号，8 号与 9 号，12 号与 13 号，17 号与 18 号，17 号与 19 号。

把距离为 1 的点合成一类，就得到新的类，把这些新类用实线圈

起来，如图 2.6.2，分别记为 G_1，G_2，…，G_5。

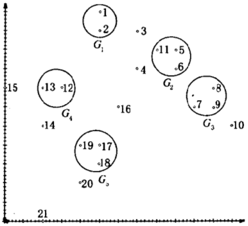


图 2.6.2

第二，以两个类中点的最短距离作为两个类的类间的距离。可计算得目前两个类间的最短距离为$\sqrt{2}$。此处 4 号墓与 G_2 中的 11 号墓距离为$\sqrt{2}$，因而 4 号墓与 G_2 的距离为$\sqrt{2}$。同样，10 号墓与 G_3 的距离，20 号墓与 G_5 的距离都是$\sqrt{2}$。把距离不大于$\sqrt{2}$的类归为一类，则得到新的类，如图 2.6.3 中实线所圈的集合。

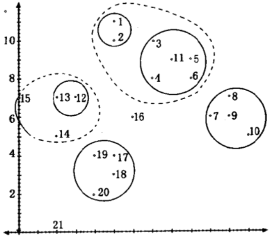


图 2.6.3

第三，仍以两个类中点的最短距离作为两类之间的距离，则现在

两个类间的最小距离为 2,将类的距离小于 2 的类合并成新类。在图 2.6.3 中新的类用虚线围成。现在,除去 16、21 这两点外,所有的点全在这 4 个类中。

3. 层 次 分 析

在错综复杂的情况下,人们期望利用各种信息作出最好的选择。如用人单位期望挑选到最优秀的人材,高中毕业生期望填报最合适的大学和专业,顾客期望选择最满意的商品等等。讨论这些问题时,所要考虑的因素很多,而且有些因素可以量化,有些因素只能作定性分析。层次分析法是将这类问题转化为定量问题,并对各种方案予以科学评价的有效方法。

层次分析法的基本步骤如下。

(1) 建立层次结构模型,将问题所要考虑的诸因素分成不同的层次

例 1 (购物模型)某一顾客要选购电冰箱。假设此时市场上有 A、B、C、D 四种电冰箱正在出售,作为评估依据该顾客考虑了八项准则:(品牌)信誉、型号、价格、容量、耗电量、制冷级别、噪音和售后服务等。经过分析各种因素的相互关系,对该顾客选择电冰箱的问题可化为如图 2.6.4 所示层次分析模型:

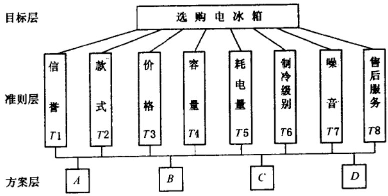


图 2.6.4

这里把所有要考虑的因素分为三个层次：目标层、准则层和方案层。目标层表示所要解决的问题；准则层表示为达到目标所要考虑的若干因素；方案层表示在这些准则下各种具体可能的选择。

例 2 （招聘干部模型）假设某公司要招聘一名干部。应聘者有三人：y_1、y_2、y_3。设该公司招聘干部的标准有五个方面：品德、才能、资历、年龄和群众关系。经过对该问题的思考，可构造如下的层次分析模型（图 2.6.5）。

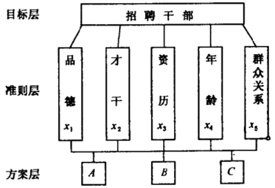


图 2.6.5

(2) 构造两两比较矩阵

现在我们以例 2 来说明两两比较矩阵的含义和作法。招聘干部考虑 5 个因素（准则）：品德 x_1，才能 x_2，资历 x_3，年龄 x_4 和群众关系 x_5。

我们要确定它们（准则）对上一层目标（招聘干部）的重要性。具体地说，我们将用量化的权重表示这些准则对上一层目标的重要性程度，即要确定品德 x_1 在招聘干部的目标中占百分之几；才能 x_2、资历 x_3、年龄 x_4 和群众关系 x_5 在招聘干部的目标中分别占百分之几？在实际生活中人们习惯于作两个事物的对比，在求权重时我们也用两两比较的方法将各因素重要性数量化，即在 5 个准则 x_1，$x_2 \cdots x_5$ 中分别比较每两个相对于招聘干部（目标）的重要性。

任取两个因素，设为 x_1（品德）与 x_2（才能），我们用正数 a_{12} 表示 x_1 相对 x_2 的重要性之比。a_{12}的值可以在数字 1，2 … 9 及其倒数

$\frac{1}{2}$，$\frac{1}{3}$ … $\frac{1}{9}$中选取。其意义是

x_i 比 x_j	相同	稍重要	重要	很重要	绝对重要
a_{ij}	1	3	5	7	9

还可以插入中间状态，即 a_{12} 还可取值 2、4、6、8。如果一个决策人认为对招聘干部来说，x_1（品德）与 x_2（才能）有差不多重要性，只是前者稍稍重要一点，他可以取 $a_{12}=2$。此时，他的选择也意味着 x_2（才能）相对 x_1（品德）而言，其重要性稍稍低一点。他同时应该取 $a_{21}=\frac{1}{2}$。同样我们把 x_1 和 x_3 比较，可以得到 a_{13} 和 a_{31}。由全部两两比较的结果可以写成下面矩阵的形式，这个矩阵就称作两两比较矩阵。例如，根据某个决策人的比较，得到如下一个两两比较矩阵：

$$\begin{pmatrix} 1 & 2 & 7 & 5 & 5 \\ \frac{1}{2} & 1 & 4 & 3 & 3 \\ \frac{1}{7} & \frac{1}{4} & 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{5} & \frac{1}{3} & 2 & 1 & 1 \\ \frac{1}{5} & \frac{1}{3} & 3 & 1 & 1 \end{pmatrix}$$

矩阵中的 a_{ij}（矩阵中第 i 行、第 j 列位置上的数）表示的是（相对招聘干部来说）第 i 个因素相对第 j 个因素的重要性。例如第一行第四列的数为 5，说明该决策人认为 x_1（品德）比 x_4（年龄）重要。

(3) 一致性检验问题

如果决策人对 5 个因素的比较具有逻辑上严格的一致性，则不会出现任何矛盾。这时他的心目中每个因素有一个重要性指标，例如 x_1 的重要性指标为 w_1，x_2 的重要性指标为 w_2，…，x_5 的重要性指标为 w_5。而 a_{12} 恰恰为这两个因素重要性指标的商，即

$$a_{12} = \frac{w_1}{w_2}$$

a_{ij}恰恰为因素 x_i 和因素 x_j 重要性指标的商，即

$$a_{ij} = \frac{w_i}{w_j}$$

这时 x_i 相对 x_j 的重要性(a_{ij})与 x_j 相对 x_k 的重要性(a_{jk})的乘积应该等于 x_i 相对 x_k 重要性(a_{ik})，这是因为

$$a_{ij} \cdot a_{jk} = \frac{w_i}{w_j} \cdot \frac{w_j}{w_k} = \frac{w_i}{w_k} = a_{ik}$$

即对任何 i, j, k，总有下列等式：

$$a_{ij} \cdot a_{jk} = a_{ik} \qquad ①$$

满足上述要求的两两比较矩阵称为一致矩阵。由于人的思维活动不可避免地带有主观性和片面性，人们构造的两两比较矩阵常常不是一致矩阵，实际极可能出现对某些 i, j, k, $a_{ij} \cdot a_{jk} \neq a_{ik}$ 的情况。因此，在分析 x_1, x_2, x_3, x_4, x_5 对招聘干部的影响时，必须对两两比较矩阵进行一致性检验。

按一致矩阵的要求逐个验证①中等式是非常不方便的事。另一种方法是计算矩阵的所谓"最大特征值"。数学理论证明：如果 n 行、n 列的两两比较矩阵是一致矩阵的话，这个矩阵的最大特征值就等于 n。至于最大特征值的含义和计算方法，我们建议读者参看有关高等代数的参考书。有些计算机软件也常常包括计算矩阵最大特征值的现成程序。

因此，只需计算一个矩阵的最大特征值就可判断该矩阵是否一致矩阵。如果矩阵不具有一致性，数学上可以证明它的最大特征值一定大于 n。而且它的最大特征值比 n 大得越多，不一致程度就越严重。这时就要重新审视两两比较矩阵，加以适当的修改，直至达到满意的一致性为止。如果它的最大特征值与 n 的差不太大，说明矩阵的不一致程度不太严重，这时我们可以认为矩阵基本上满足了一

致性要求。从理论上说，通常的一个矩阵，只有很少的例外是严格满足一致性要求的。

可以计算得例 2 中的两两比较矩阵的最大的特征值为 5.072，这说明该矩阵不是一致矩阵，但它的不一致性程度是可接受的，我们认为它具有满意的一致性。

(4) 各因素权重的计算

在确认两两比较矩阵

$$\begin{pmatrix} 1 & 2 & 7 & 5 & 5 \\ \frac{1}{2} & 1 & 4 & 3 & 3 \\ \frac{1}{7} & \frac{1}{4} & 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{5} & \frac{1}{3} & 2 & 1 & 1 \\ \frac{1}{5} & \frac{1}{3} & 3 & 1 & 1 \end{pmatrix}$$

满足一致性要求(或它的不一致性是可以接受的)以后，我们可以计算相应的因素对目标(招聘干部)的权重。方法是：

将矩阵同一行的 5 个数相加，例如第一行的 5 个数字之和为

$$1+2+7+5+5=20$$

各行数字之和依次为

$$20,\ 11.5,\ 2.226,\ 4.533,\ 5.533$$

其总和为 43.792，用 $\frac{20}{43.792}=45.67\%$ 刻画第一个因素的权重。按此计算得各个因素在目标中所占的权重，见下表：

因　素	x_1	x_2	x_3	x_4	x_5
权重(%)	45.67	26.26	5.08	10.35	12.64

这些权重反映了决策者招聘干部时，认为品德条件最重要，其次

是才能，再次是群众关系、年龄因素，最后才是资历。

(5) 决策方法

现在希望从三个应聘者 y_1，y_2，y_3 中选一个在总体上最适合上述五个条件的应聘者。为此，对三个应聘者分别比较他们的品德(x_1)，才能(x_2)，资历(x_3)，年龄(x_4)和群众关系(x_5)。例如先两两比较三个应聘者的品德，得两两比较矩阵

$$B_1 = \begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{8} \\ 3 & 1 & \frac{1}{3} \\ 8 & 3 & 1 \end{pmatrix}$$

上式的第一行第二列的元素为$\frac{1}{3}$，表示以品德来说，第一个应聘者比第二个应聘者稍差一些。矩阵内其他位置上的数也表示了相应的应聘者品德比较的结果。

经计算，可知矩阵 B_1 的不一致程度可接受。按上述计算权重的方法计算得，对 x_1(品德)而言，三个应聘者的权重分别为

$$0.082,\ 0.244,\ 0.674$$

类似地，分别比较三个应聘者的才能、资历、年龄、群众关系，分别得到两两比较矩阵

$$B_2 = \begin{pmatrix} 1 & 2 & 5 \\ \frac{1}{2} & 1 & 2 \\ \frac{1}{5} & \frac{1}{2} & 1 \end{pmatrix}$$

$$B_3 = \begin{pmatrix} 1 & 1 & 3 \\ 1 & 1 & 3 \\ \frac{1}{3} & \frac{1}{3} & 1 \end{pmatrix}$$

$$B_4 = \begin{pmatrix} 1 & 3 & 4 \\ \frac{1}{3} & 1 & 1 \\ \frac{1}{4} & 1 & 1 \end{pmatrix}$$

$$B_5 = \begin{pmatrix} 1 & 1 & \frac{1}{4} \\ 1 & 1 & \frac{1}{4} \\ 4 & 4 & 1 \end{pmatrix}$$

通过计算知，相对 x_2 而言，三个人的权重分别为

$$0.606,\ 0.265,\ 0.129$$

相对 x_3 而言，三个人的权重分别为

$$0.429,\ 0.429,\ 0.142$$

相对 x_4 而言，三个人的权重分别为

$$0.636,\ 0.185,\ 0.179$$

相对 x_5 而言，三个人的权重分别为

$$0.167,\ 0.167,\ 0.666$$

它们可分别视为各应聘者的才能分、资历分、年龄分和群众关系分。

把各人各因素（准则）得分和各因素在总目标（招聘干部）中的权重联系起来，可以得到各应聘者的总得分。例如 y_1 的总得分为

$$\begin{aligned} & 0.4567 \times 0.082 + 0.2626 \times 0.606 + 0.0508 \times 0.429 + \\ & 0.1035 \times 0.636 + 0.1264 \times 0.167 \\ = {} & 0.3053 \end{aligned}$$

以上总得分实际上是诸因素得分的加权平均值。这里的权就是

各因素 x_i 相对于目标(招聘干部)重要性的权重。同理可得 y_2，y_3 的得分分别为 0.243 1、0.452 6。由比较得分的多少,可以推出:应聘者 y_3 是此次选拔干部的第一人选。

第七节　算法:从验血方案谈起

计算机的计算速度之快,远远超出了人们的想象,每秒运算一亿次的计算机已经十分平常。但是从解决数学问题的要求来看,有时还是嫌它太慢了。一亿次是 10^8,一年约 3.2×10^7 秒,所以即使计算机不停的运行,一年也只能运算 3.2×10^{15} 次。如果一个数学问题要计算 30!,而 $30!\approx2.6\times10^{32}$,这就是说,对于 30!,要计算机不停地计算 8.0×10^{16} 年,这是难以接受的。因此,即使是计算机时代,计算的复杂程度仍然是我们必须面对的数学问题。

1. 从几个例子看计算复杂性

例 1　(验血问题)某次大战前夕,10 万大军将在三天后出征。军医发现军中有一位士兵带入了一种传染病菌。三天后发作将快速传染全军,使十万大军丧失战斗力,只有验血才能判断谁是患者。当时军医每天最多能检验血样 100 份,如果逐一验血,至少需要1 000 天,这将延误军机,将军求教专家,一数学家提出一种方案,顺利地解决了这一问题。

方法是将 10 万人分成 100 组,每组 1 000 人,滴血于一处,当天将此 100 份血样交验,必有且仅有一份血样含有病血;第二天,将这份病血中的 1 000 人分成 100 组,每组 10 人,取样验血,同样必有一份且仅有一份血样有病血;第三天,将有病血这一组的 10 人逐一抽血化验,即可确定患者,再给他服药,即可保证全军准时出征。

一般地说,如果全军有 x 人,用 $\{x\}$ 表示对 x 取上整,则对全军逐一检验需要的天数是 $\left\{\frac{x}{100}\right\}$,而用上述数学家的方法需要的天数

只是 $\{\log_{100}x\} = \left\{\frac{1}{2}\log_{10}x\right\}$。

当 $x = 100\,000$ 时，$\left\{\frac{1}{2}\log_{10}x\right\} = \left\{\frac{5}{2}\right\} = 3$，而 $\left\{\frac{x}{100}\right\} = 1\,000$；当 $x = 1\,000\,000$，$\left\{\frac{1}{2}\log_{10}x\right\} = \left\{\frac{6}{2}\right\} = 3$，而 $\left\{\frac{x}{100}\right\} = 10\,000$。显然 $\left\{\frac{1}{2}\log_{10}x\right\}$ 比 $\left\{\frac{x}{100}\right\}$ 小得多了。对于这样一类特殊的问题，分析问题的实质，迅速找出其解，国际上称这种特殊的检验方法为群验法(group testing)。

这个例子说明，解决问题时，方法的"好"、"坏"、"快"、"慢"是十分重要的。

例 2 （中国邮递员问题）邮递员从邮局取出信件，沿街投递，走遍投递范围的每一条街道，然后返回邮局。他如何选择一条尽可能短的投递路线？这是我国数学家管梅谷首先提出并进行研究的，国际上称为中国邮递员问题。

我们把邮局和交叉路口看成"点"，连接这些"点"的街道看成"边"，这些街道的长度称为该边的"权"，从而得到一个网络 G。与网络中的点"关联"的边的条数称为该点的次，次为奇数的点称为"奇点"，否则称为"偶点"。

解决中国邮递员问题的最早算法是"奇偶点图上作业法"，它可以归结为如下口诀："先分奇偶点，奇点对对连，连线不重复，重复需改变，圈上连线长，不得过半圈，连线超半圈，对换连线边"。

例如某邮递员负责投递邮件的街道如图 2.7.1 所示，求最短投递路线。

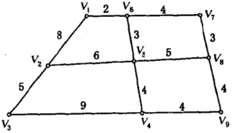


图 2.7.1

该网络有四个奇点 V_2、V_4、V_6、V_8，将 V_2 与 V_4 看成一对，V_6 与 V_8 看成一对，添加连线后成为图 2.7.2：

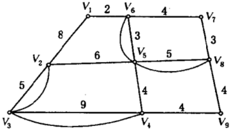


图 2.7.2

由于圈 $V_2V_3V_4V_5V_2$ 圈长之和为 24，其中连线 V_2V_3 和 V_3V_4 的长度之和为 14，超过圈长的一半，于是可去掉连线 V_2V_3 和 V_3V_4，增加连线 V_2V_5 和 V_5V_4。

同样对圈 $V_6V_5V_8V_7V_6$，连线 V_8V_5 和 V_5V_6 的长度之和 8，大于圈长 15 的一半，删除连线 V_8V_5，V_5V_6，增加连线 V_6V_7 和 V_7V_8，得图 2.7.3 为最短投递路线。

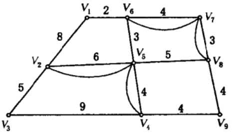


图 2.7.3

对图 2.7.3 用上述口诀进行检验：连线最多出现一次，每一圈的连线长不超过该圈的一半。如果把邮局设在 V_1，则最短投递路线为：$V_1V_2V_3V_4V_5V_2V_5V_4V_9V_8V_5V_6V_7V_8V_7V_6V_1$。

这个算法需要对每一个圈进行检验，在计算机上实现是困难的。1973 年 Edmonds(爱德蒙斯)和 Johnson(约翰逊)提出一个快速算法求解中国邮递员问题。

例 3 (旅行售货员问题)如果邮递员投递的是国际快件，选择

最短投递路线,从邮局出发经过一组顾客中的每一位的住处再返回邮局使总的行程最短,这就是有名的旅行售货员问题(简称为 TSP (Travelling Salesman problem))。这个问题又可以叙述为:从 n 个城市中的某一个城市出发到其他 $n-1$ 个城市推销产品,要求每个城市到达一次且仅一次,再回到原出发城市,问如何选择旅行路线,使总的行程最短。类似地,某些生产自动线加工顺序问题也可以归结为这类问题。对这类问题已有的精确解法,本质上都是要枚举可能的各种情况。

2. 计算复杂程度的界定

从以上例子可以看出:许多实际问题往往是在有限个可行方案中,选择一个"最优"的结果。表面上看来,从有限个可能的情况中选择一个满意的方案是很简单的,只要逐一数遍即可,然而事实上并不如此简单。一个问题的算法,如果需要计算几个月,几年甚至更多,实际上是行不通的。例如旅行售货员问题,当投递快信 20 封时,可能的选择方案就有 $\frac{20!}{2}=1.211\,645\,1\times10^{18}$ 种。假定计算机运算一次就可得到一种投递方案的行程长度,以每秒进行 100 亿次运算的计算机求解,也需要 4 个半月。因此对于一些理论上可以求最优解的问题,不能简单地认为它已经解决了。

为了讨论方便起见,我们假定计算机的存贮量足够大,运算时间任意长,计算精度也足够保证问题的要求,这样"理想"的计算机称为图灵机(Turing Machine)。在图灵机上解题,计算时间的长短主要与以下因素有关:

1) 计算机的速度;

2) 实际问题规模的大小;

3) 算法的选择。

如果研究的问题,其规模 n 是确定的,此时解题所需的时间主要与计算机的速度和选择的算法有关。

设 A 是解决问题 D 的一种算法，以 $f_A(D, n)$表示用算法 A 求解规模为 n 的问题 D 所需的运算次数。

要缩短运算时间或在一定时间内能解更大规模的问题，其主要办法为：提高计算机的速度和改进算法，减少运算次数。

首先考虑前者的影响，如果现有的计算机每小时解题的规模为 N，用快 100 倍，快 1 000 倍的新计算机，一小时所能解决问题的规模，如何变化，请看下列表格：

算法复杂性	解题规模 n 的变化		
	现有计算机	计算机快 100 倍	计算机快 1 000 倍
n	N	$100N$	$1\,000N$
n^2	N	$10N$	$31.6N$
n^3	N	$4.64N$	$10N$
n^5	N	$2.5N$	$3.98N$
2^n	N	$N+6.64$	$N+9.97$
3^n	N	$N+4.19$	$N+6.29$

从上述表格中，可以看出：算法复杂性为规模 n 的多项式时，计算机成倍提速后，相应地解题规模也成倍增长；对算法复杂性为指数函数的算法，例如 $f_A(D, n)=3^n$ 时，计算机提速 1 000 倍后，解题规模 n 只能增加 6.29。所以对指数函数的算法，单纯靠计算机提速来增加解题的规模 n 的收效甚微，因此转向算法的研究是必要的。

首先对算法进行分类：

如果存在一个多项式 $P(n)$和正整数 n_0，使得当 $n>n_0$ 时，恒有 $f_A(D, n)\leqslant P(n)$，则称 A 为解决问题 D 的多项式算法，又称为有效算法，或好算法。前面介绍的验血问题的解法和中国邮递员问题的 Edmonds-Johnson 算法，都是求解相应问题的多项式算法。

如果 $f_A(D, n)$是 n 的指数函数，则称算法 A 为解决问题 D 的指数型算法。例如求解中国邮递员问题的“奇偶点图上作业法”是指数型算法。指数型算法又称为“坏”算法或“无效”算法。

对于一个算法复杂性为 n^{80} 的问题，虽然是多项式算法，但实际

上也是不可接受的。因为 $2^{80} \approx 10^{24}$，对这样"天文"数字，现实情况下，计算结果几乎是不可能的。幸运的是一个实际问题一旦找到多项式算法，经过一系列的改进，其算法复杂性会降到 n 的三次多项式，甚至可能降到次数更低的多项式。因此有理由相信多项式算法实用上是有效的。

由于我们定义的算法复杂性是考虑所有可能情况下，算法的运算次数。排除"最坏情况"的一些指数型的算法也被人们广泛采用，例如求解线性规划的单纯形法，已经证明它是指数型的算法，"最坏"情况的出现是极其罕见的，算法的平均运算次数是规模 n 的多项式。大多数的指数型算法，只是穷举搜索法的变种，只有对问题的结构充分了解后才能给出多项式算法。解决一个实际问题时，首先寻求多项式算法，如果一个问题确实没有多项式算法，而你再去寻找，精力就白费了，因此有必要对实际问题进行分类。

3. P 问题和 NP 问题

对于一个实际问题，如果其存在多项式算法，则称为 P 问题 (Polynomial Problem)。对 P 问题，研究的中心问题是如何改进现有的计算方法使运算次数更少。

对于一个实际问题，如果已经证明不存在多项式算法，我们认为这一个问题是难问题。对于难问题，一般只能寻找枚举的办法或寻找可以接受的近似算法。

还有一类实际问题，称为判定问题；是能用"是"(有)或"不"(无)来回答的问题。例如，问用 2 500 元能够购置 29 英寸的彩色电视机吗？回答这个问题"能"时，不必知道当前市场上，29 英寸彩电的最低价，只需了解确有价格不超过 2 500 元的 29 英寸彩电出售即可。

对于一个判定问题，如果对所有回答为"是"的实例，都存在多项式算法来验证它的正确性，则称此判定问题为 NP 问题(不确定多项式问题，non-deterministic polynomial problem)显然 P 问题一定是 NP 问题。

1971年库克(Cook)发表了一篇十分著名的论文《The complexity of theorem-proving, Association of Computing Machinery》。他首先指出,NP问题中存在一类称为NPC的问题(NPC—完备问题,non-deterministic polynornial complete problem)。这类问题有如下特性:

1) 类中每一个问题至今尚未找到多项式算法;

2) 如果类中任一个问题有多项式算法,那么该类中其他问题都有多项式算法(即这类中的任意两个问题都存在多项式算法相互转化)。

到目前为止,NPC问题已被扩充为近千个,其中包括旅行售货员问题。许多优秀的数学家、理论计算科学家在过去几十年来,试图寻找它们的多项式算法都没有成功,这越来越使人们相信,对它们也许根本不存在多项式算法。然而要证明这一猜想,既是有重大意义的,又是十分困难的。2000年5月24日Clay数学所宣布七个"千禧年数学难题",每一个悬赏一百万美元征解,其中的第一个问题就是这个猜想。这个猜想的解决实属渺茫,有理由相信,不提出一套全新的数学理论和方法,这个问题的答案是不会出现的。在历来的研究中,一个问题一旦被证明是NPC问题,通常人们就放弃追寻多项式算法。

由于NP问题的解有重大的实际意义,而精确求解又极其困难,这就迫使人们寻找解决这类问题的策略,下面介绍一些实践中行之有效的算法:

1) 近似算法。通常这是多项式算法,给出的解往往不是最优解(精确解),但能保证与最优解的误差在给定的范围内。

2) 概率算法。对某些分类问题或识别问题,可以假设其中的参数为满足某种概率分布的随机变量,这样可能设计出一种在通常的计算实践中不错的算法。

3) 特例法。对某些NPC问题的特殊情况,有时可以设计一些特殊的有效算法。

4) 指数算法。有些算法尽管在最坏情况下,其算法复杂性为规

模 n 的指数函数，但在实际中最坏情况下很少产生，例如解线性规划的单纯形法。

5）局部求优法。这一类算法的基本思想是用局部最优解来代替整体最优解。首先选择一个较“好”的初始可行解和它的“领域”制定一种搜索方案，求得该领域内的最优解并以此来代替原问题的最优解，“领域”的选择，通常是凭经验和直觉。

6）启发式算法，上述五种方法就思路而言，都可以看成某种启发式算法。启发式算法通常是凭经验或对事物的观察作出决策，从严格的数学理论的要求来看，不能令人满意，但在实践中往往是有效的。

第八节　对策论的例:田忌赛马

竞争是当代社会的一个特征。在竞争中讲究科学的对策是十分重要的。经济活动中的经营决策、市场竞争,政治活动中的竞标、竞选、谈判、联盟,军事活动中对抗、谋略等都和选择合适的对策有关。20世纪四、五十年代创立的对策论(又称博弈论)研究了一系列社会经济中的对策问题。此处我们介绍其中一些最简单的对策问题。

1. 田忌赛马的故事

田忌赛马是一个非常有名的谋略故事。传说战国时代齐国的齐威王经常与大将田忌赛马。赛马的规则是这样:每次双方各出三匹马,一对一共比赛三个回合,每个回合的输方要给赢方铜一千斤。齐威王的三匹马和田忌的三匹马按实力强弱都可分为上、中、下三等。齐威王的上、中、下三匹马分别比田忌的上、中、下三匹马略强一些。因此每次赛马田忌都是连输三个回合,都要输掉铜三千斤。后来田忌手下的谋士孙膑给田忌出了个主意,要田忌用他的下马和齐威王的上马比赛,用他的上马和齐威王的中马比赛,用中马和齐威王的下马比赛。这样,虽然第一回合田忌必输无疑,但田忌却赢了后面的两个回合,二胜一负,田忌赢了齐威王铜一千斤。同样的马,输赢却发生了变化。这个故事说明了策略的重要性。在双方实力、条件不变的情况下,适当地调度和运用现有的条件会取得更好的结果。

这个故事中的齐威王实际上把自己放在一个不公平的地位上。因为他自持实力强大,总是先出马,给了田忌采取有利的对策的机会。如果他每次比赛以前能放下国君的架子谦让一下:“田先生,您

先请”，也许又是他连赢三场了。

公平比赛条件应该是：齐威王和田忌双方都清楚各自马的实力和对方马的实力，每个人都可以按自己的意愿决定自己马匹出场的次序，而两人出马的对策应该是同时的，不能总让某个人先出马。

这时，对齐威王来说，最理想的情况是：各回合的马匹与田忌所出的马匹等级都相同，即不管先后次序如何，总是以自己的上马比田忌的上马，以自己的中马比田忌的中马，以自己的下马比田忌的下马，这样他总能赢铜三千斤。次佳的是：三场中有一场是同等级的马比赛，例如齐威王的下马对田忌的下马（齐威王赢），而上马、中马要和田忌的中马、上马比，此时齐威王的上马必赢，三场比赛齐威王至少两胜一负。对齐威王来说，最坏的情况是故事中孙膑所建议的对策：齐威王的上、中、下马分别对田忌的下、上、中马，一胜二负，最终要输铜一千斤。

为了把齐威王与田忌赛马的故事引伸成一个对策问题，我们先把双方出三匹马简化成各出两匹马，分别称为上马、下马。问题的假设如下：

1）该对策问题中有两方，即齐威王和田忌；

2）双方可选择的对策是己方马匹的出场次序，由于两匹马的排列次序共有 $2! = 2$ 种，因此每一方各有 2 种可选择的对策；

3）双方都预先知道对方所有可能的对策，并且预先知道双方每一种对策组合的结果；

4）在比赛之前双方都不能预先知道对方究竟会采取什么对策，双方同时选择对策，没有先后次序关系，而且一场比赛的对策一旦选定就不允许变更；

5）把赢铜一千斤记收益为“1”，输铜一千斤记收益为“－1”，则对策的一方齐威王在各种对策组合下的收益如下表所示：

齐威王的收益表

		田忌	
		上下	下上
齐王	上下	2	0
	下上	0	2

表中的数字是在比赛双方采取相应对策时齐威王的收益。齐威王的收益就是田忌的损失，因而把表中的数字全部改变符号后就可以得到田忌的收益。那么在这个对策问题中齐威王和田忌会怎样选择自己的对策，而最终的结果又会是怎样的呢？

为了回答这些问题，我们先来看看问题有什么特点。

首先，由前面的分析可知，双方都不能让对方知道或猜中自己的对策，因为一旦自己的对策被对方知道，则对方就可以有针对性地采取适当的对策，自己就处于不利的地位。这也意味着任何一方的选择不能一成不变，对策的变动以使得对方无法预测为好。这就意味着选择对策必须要有一定的随机性。其次，无论对齐威王还是对田忌，两种可选择的对策相互之间没有优劣之分。如对齐威王来讲，每一种对策都可能有两种可能的结果，包括一种收益为 2，一种收益为 0。实际究竟得到哪种结果，要看双方对策的组合情况，而不仅取决某一方的对策。同样对田忌来说，他的两种对策也无好坏之分，每种对策也有两个可能的结果，可能的收益为 0 或 −2。总之，比赛双方在选取对策时对己方的可选对策并无偏爱，应以相同的可能性选用。实际上，偏向于某种对策的结果往往对自己不利，因为当对方得知你的偏爱后就可以针对性选择对策，从而有更多的机会取得有利的结果。这种对策游戏如果只进行一次，则双方的选择和最终的结果都无法确定，完全只能靠运气。由于齐威王的马的实力比田忌的马略高，他赢的机会比田忌要大得多。如果这样的对策游戏重复进行多次，则上面的讨论给我们指出了各方选择对策的原则，而且进一步讨论还能告诉我们多次比赛后的平均结果。这种对策问题称为随机对策问题，我们可以应用平均数来作计算。计算的方法如下。

表中各种对策组合出现的可能性都相同，概率都等于 0.25。由表中数据，齐威王的收益为 0 和 2 的概率都是 0.5。于是齐威王的平均收益为

$$0\times0.5+2\times0.5=1$$

即齐威王和田忌若按随机对策方法赛上下两匹马，则齐威王平均每次赢田忌一千斤铜。

2. 均 衡 对 策

例 1 假设某地区有两家电视台，在同一天的同一个黄金时间，每家各有两套节目可供选择播出。经调查，两家电视台各种节目搭配时甲台节目收视率如下表：

甲台节目收视率(%)

		乙台	
		节目 1	节目 2
甲台	节目 A	70	40
	节目 B	55	45

表中只列出了甲台节目的收视率，乙台节目的收视率可以由以下的公式得到：

$$乙台收视率 = 100\% - 甲台收视率$$

这里我们假设该地区的观众不是收看甲台的节目就是收看乙台的节目。我们还假设两家电视台事先都知道这张表，即他们都知道彼此的情况和选用各种节目后的结果，并且在播放过程中可以调整播放的节目。我们要分析这两家电视台会播放什么节目，即他们会采取什么对策来面对他们之间的竞争呢？

如果甲台播放节目 A，期望得到 70%的收视率；但是此时乙台会播放节目 2，使甲台只能得到 40%的收视率。而甲台播放节目 B，则不管乙台播放什么节目，最少可得到 45%的收视率。两者相比，必然是甲台播放节目 B，乙台播放节目 2。由此推知，甲台的收视率将为 45%，乙台的收视率将为 55%。

现在转到从乙台的立场来考虑问题。我们先把上面的表转换成乙台节目收视率的表：

乙台节目收视率(%)

		乙台	
		节目 1	节目 2
甲台	节目 A	30	60
	节目 B	45	55

如果乙台播放节目 1,最多得到 45%的收视率。但此时甲台会播放节目 A,使乙台只得到 30%的收视率。乙台播放节目 2,则最多可得到 60%的收视率,但是此时对甲台最好的选择是播放节目 B,使乙台只得到 55%的收视率。两者相比,必然是乙台播放节目 2,甲台播放节目 B。甲台的收视率将为 45%,乙台的收视率将为 55%。所得的结果和前面分析的结果相同。

例 2 如果两家电视台可能播放的节目分别为四个、三个。甲台节目收视率(%)如下表所示:

甲台节目收视率(%)

		乙台		
		节目 1	节目 2	节目 3
甲台	A 节目	70	50	35
	B 节目	45	40	50
	C 节目	55	50	55
	D 节目	60	45	50

此时情况变得比较复杂,我们又如何分析他们的对策呢? 分析的思想方法仍和例 1 相同,可以用下表表示。

基于甲台节目收视率的对策分析表(%)

		乙台			
		节目 1	节目 2	节目 3	$a = 50$
甲台	A 节目	70	50	35	35
	B 节目	45	40	50	40
	C 节目	55	50	55	50
	D 节目	60	45	50	45
	$b = 50$	70	50	55	$c = 50$

表中的第6列(最后一列)的数字是同一行数字中最小的数字。例如表中第三行对应甲台节目 A 的最后一个数字是35,它是70、50、35三个数字中的最小的数字,我们称之为甲台节目 A 收视率的保守估计。这个数字表示当甲播放节目 A 时,不管乙台播放什么节目它所能得到的最低的收视率。而在这一列上面的第一个数字 $a(=50)$,是最后一列对应甲台各节目收视率保守估计中的最大的数字。a 表示在甲台所有可能的选择中,可以得到保证的最高的收视率。表中的最后一行的各数是同一列数字中的最大的数字。例如该行的第三个数字是50,它是50、40、50、45四个数字中的最大数字。这个数字对应乙台播放节目2时的情况,说明当乙台播放节目2时,只要甲台应对得当(此时甲应该播放节目 A 或节目 C),甲台所能够得到的最高收视率。我们称这个数字为乙台播放节目2时甲台收视率的最乐观估计。该行的第一个数字 $b=50$ 是这一行中最小的数字。表示的是对乙台所有可能的选择,只要应对得当,甲台能获得的最低的收视率。在右下角的数字 c 是与 a、b 相等的数,这里是50。对应这个数字的是甲台播放节目 C,乙台播放节目2,各获得50%的收视率。这就是两家电视台都会采取的科学对策。我们称这种决策为均衡对策组合。

下面我们可以试试其他对策组合会发生什么情况。结论将是:改变这样的选择将使改变者的收视率降低,从而双方都不会采用除此以外的其他对策。这也是称此决策为"均衡对策"的原因。

假设甲台不是播放节目 C,而是播放节目 A,期望得到更高的收视率(70%);此时乙台会播放节目3,使甲台只能得到35%的收视率,比均衡对策组合中甲的收视率(50%)低。另一方面,如果乙台不是播放节目2,而是播放节目3,期望得到更高的收视率(65%);则此时甲台会播放节目 C,使得乙台只得到45%的收视率,低于均衡对策组合50%的收视率。其他对策组合也将有同样的结果,从而证实了上述的结论。因而甲台播放节目 C,乙台播放节目2是双方都能接受的结果。

在对策论中,这样的模型称为"两人零和对策"。这是因为:如果

把两人中输的一方记为－1，赢的一方记为1，则他们的和为零。其实如果每种对策组合的结果都是一个与对策组合无关的常数，也都可以作为零和对策。例如上述电视台的收视率总和恒为1，也属于零和对策。两人零和对策是对策论中所研究的许多问题中的一个。按照这种方法计算得到的 a 和 b，在有些情况下是不相等的，这时我们就称该对策问题为不稳定对策问题；相应地，a 和 b 相等时的对策问题称为稳定的对策问题。例2是一个稳定对策问题。在稳定对策问题的情况下，一般情况也像例2中分析的那样，会有一个双方都可接受的对策组合，任何一方改变对策，只会使自己的利益受损。用这种方法计算例1的情况，得到同样的结论，这也是一个稳定的对策问题。下面我们举一个不稳定对策问题的例子。

例3 两家电视台各种节目搭配时的甲台节目收视率如下表：

甲台节目收视率(%)

		乙台	
		节目1	节目2
甲台	节目 A	70	40
	节目 B	45	55

用上述方法对此例进行计算，得到表格如下：

		乙台		
		节目1	节目2	$a=45$
甲台	节目 A	70	40	40
	节目 B	45	55	45
	$b=55$	70	55	$a\neq b$

由表中可知，$a\neq b$。我们来具体看看一方播放某个节目后会有什么情况发生：如果甲台播放节目 A，以期得到70%的收视率，此时乙台一定不会播放节目1，而是播放节目2，这样对乙台来说，可以获得60%的收视率。但若乙台播放节目2，甲台必然改播节目 B，以获得55%的收视率。但若甲台播放节目 B，乙台必然改播节目1，以获得

55%的收视率。但若乙台播放节目 1，甲台必然改播节目 A，以期获得 70%的收视率……这样看来每种对策组合都不能使双方同时满意。这就是为什么称这样的对策问题是“不稳定”的原因。

3. 随机对策和期望

让我们再回到田忌赛马的问题上，齐王和田忌也构成零和对策的双方，按处理零和对策的方法，由下表（表中的数字表示千斤铜的量）可知，在这个问题中不存在均衡策略，那么我们应如何分析和解释这个问题呢？这就需要运用随机的思想和概率的方法。

基于齐王的收益表

		田			忌			
		上中下	上下中	中上下	中下上	下上中	下中上	$a=-1$
齐王	上中下	3	1	1	1	−1	1	−1
	上下中	1	3	1	1	1	−1	−1
	中上下	1	−1	3	1	1	1	−1
	中下上	−1	1	1	3	1	1	−1
	下上中	1	1	1	−1	3	1	−1
	下中上	1	1	−1	1	1	3	−1
	$b=3$	3	3	3	3	3	3	$a \neq b$

齐王和田忌各有 6 种策略，如果比赛双方预先都不知道对方所选的策略，且各人选择每种策略的概率都是相同的，都是 1/6。那么，各人比赛结果的收益是随机的。例如当齐王出策略“上中下”时，若田忌的策略是“上中下”，则齐王赢 3 千斤铜；若田忌的策略是“中下上”，则齐王赢 1 千斤铜；若田忌的策略是“下上中”，则齐王输 1 千斤铜。由概率的知识可计算得齐王的平均得益是：

$$\bar{x}=\frac{1}{6}(3+1+1+1-1+1)=1$$

即齐王虽然每次比赛的盈利数是未知的，但是可计算得其平均

盈利是 1 千斤铜，随机数学中将这个平均数“1”称为期望值。从上表中还可看出，在齐王随机地采用其他策略时，其盈利的期望值也都是 1(千斤铜)。

在同样的比赛规则下，我们还可计算得田忌的盈利的期望值是

$$\bar{y}=\frac{1}{6}(-3-1-1-1+1-1)=-1$$

即平均输 1 千斤铜。

到现在为止，可将他们的比赛对策归纳如下：

1) 如果齐王先宣布自己的出场阵势是“上中下”，那么当田忌是笨蛋，也出“上中下”时，齐王将赢得 3 千斤铜，这是田忌的最差策略；

2) 如果齐王先宣布自己的出场阵势是“上中下”，那么当田忌是聪明人，会出它的最好策略“下上中”，齐王将输掉 1 千斤铜；

3) 如果齐王预先不宣布自己的策略，且田忌也是聪明人，他们两人都随机地调换各种策略，那么这时不存在最好策略或最差策略，田忌可能会赢 1 千斤铜，也可能会输 3 千斤或 1 千斤铜，但总体来说，田忌会平均输 1 千斤铜，而齐王会平均赢 1 千斤铜。事实上齐王的实力确实比田忌强些；

4) 如果两个人都不预先宣布自己的策略，而其中的一位又有策略偏向，即对 6 种策略不是随机应用。我们不妨假设田忌有策略偏向，例如，他糊涂地认为“下上中”的策略最可能赢，因而一直出这种策略，齐王一旦掌握了田忌的这种偏向，只要也出“下上中”的策略，田忌就会输 3 千斤铜。或者田忌只局限在几种策略中进行选择(如只选“下上中”、“下中上”和“上下中”)，而另一些策略从不选择，那么齐王只要不选针对这些策略中对自己最不利的对策(即不选“上中下”、“上下中”和“中上下”)，就可增加赢的次数和赢的铜数$\left(\text{可计算得此时齐王盈利的期望值为}\frac{13}{9}\geqslant 1\right)$。

在随机对策中，如果双方都是“聪明人”的话，不存在“必赢”的策略，都必须冒风险，但是我们必须把握机会、不犯错误，争取尽量高的期望值。

习题

1. 在“石头、剪子、布”的猜拳游戏中，石头赢剪子，剪子赢布，布赢石头。规定赢者得1分，输者不得分。比较下面几种情况，考虑对策的选择应该有何不同？

(1) 对方先出拳；

(2) 对方只出一种拳；

(3) 对方大多数出“石头”；

(4) 对方只出两种拳；

(5) 对方随意出拳。

2. 在齐威王和田忌赛马各出三匹马的情况下，有几种可能的对策组合？齐威王在所有的组合中取胜的有多少组合？占总数的比例是多少？这个比例说明什么问题(提示：考虑两人比赛次数非常多时的情况)？

3. 在两家电视台竞争的例子中，若事先每一方都不能知道对方会播放什么节目，而且假设节目一经决定就不能变动，此时两家电视台会如何决策？

4. 如果齐王和田忌都不预先公布自己的策略，但是田忌知道齐王总是把“上马”放在最后出场，那么田忌应如何对策，才能获得最大盈利？盈利为多少？

第九节　背包问题和线性规划

一个旅行者外出远游，由于负重能力的限制只能选带少量必需的日用品，选带哪些日用品最合适？为了优化牲畜品种，要在原有不同品种的牲畜中选择两个品种试行交配，怎样选择试验品种可使试验费用最小？一项综合工程需建在不同的几个地方，在可供选择的地点中如何选址才能使综合效益最佳？等等，这些问题都是规划问题。在现实生活中有许多规划问题。

1. 0—1 规划的问题

例 1　(背包问题)一个旅行者，为了准备必要的物品，要在背包里装一些最有用的东西。他共有 m 件物品，按物品有用的程度定出物品的“价值”，设第 i 件物品的价值记为 c_i，重量为 a_i，而他最多只能带 b 千克的物品。那么他应选带哪些物品，使总重量不超过 b 且使用价值最大？

由于物品只能整件带，变量 x_i 表示第 i 件物品“带”或“不带”，规定：

$$x_i = \begin{cases} 1 & \text{带第 } i \text{ 件物品} \\ 0 & \text{不带第 } i \text{ 件物品} \end{cases}$$

目标函数为：

$$y = c_1x_1 + c_2x_2 + \cdots + c_mx_m$$

问题要求的是使目标函数 y 最大的解$(x_1, x_2, \cdots, x_m)$，其中约束条件为：

$$\begin{cases} y = \sum_{i=1}^{m} a_i x_i \leqslant b \\ x_i = \{0, 1\}(i = 1, 2, \cdots, m) \end{cases}$$

例 2 （指派问题）车间里有 4 位师傅 $A_i(i = 1, 2, 3, 4)$，他们都能独立完成四项不同的任务 $B_j(j = 1, 2, 3, 4)$。由于他们各有特长，完成四项任务所需的时间不同，下面的表中列出了他们完成每项工作所需的时间。

	B_1	B_2	B_3	B_4
A_1	3	14	10	5
A_2	10	4	12	10
A_3	9	14	15	13
A_4	7	8	11	9

规定每项任务安排一人，且仅安排一人。问怎样安排才能使四项任务完成的总时间最少？

设变量 x_{ij} 表示安排 A_i 去做任务 B_j，并规定：

$$x_{ij} = \begin{cases} 1 & A_i \text{ 做任务 } B_j \\ 0 & A_i \text{ 不做任务 } B_j \end{cases}$$

每个人都有一项工作：即 $\sum_{j=1}^{4} x_{ij} = 1(i = 1, 2, 3, 4)$，

每项工作都有一人做：即 $\sum_{i=1}^{4} x_{ij} = 1(j = 1, 2, 3, 4)$。

目标函数是

$$\begin{aligned} T = {} & 3x_{11} + 14x_{12} + 10x_{13} + 5x_{14} \\ & + 10x_{21} + 4x_{22} + 12x_{23} + 10x_{24} \\ & + 9x_{31} + 14x_{32} + 15x_{33} + 13x_{34} \\ & + 7x_{41} + 8x_{42} + 11x_{43} + 9x_{44} \end{aligned}$$

$$\text{约束条件为}\begin{cases}\sum_{j=1}^{4} x_{ij} = 1 \\ \sum_{i=1}^{4} x_{ij} = 1 \\ x_{ij} = \{0,\ 1\}\ (i,\ j = 1,\ 2,\ 3,\ 4)\end{cases}$$

问题是要求使目标函数 T 最小的解 $\{x_{ij} \mid i,\ j = 1,\ 2,\ 3,\ 4\}$。

例 3 (选址问题)某公司准备在市东、西、南三个区建立门市部,有 7 个点 $A_i(i = 1,\ 2,\ \cdots,\ 7)$ 可供选择。要求

(1) 在东区,A_1, A_2, A_3 三个点中至多选两个;

(2) 在西区,A_4, A_5 两个点中至少选一个;

(3) 在南区,A_6, A_7 两个点中至少选一个。

如果选用 A_i 点,设备投资费用为 b_i 元,每年可获利润 c_i 元,而投资总额不得超过 B 元。问如何选点可使年利润为最大?

若以变量 x_i 表示 A_i 是否被选用的变量,规定:

$$x_i = \begin{cases}1 & A_i\ \text{被选用} \\ 0 & A_i\ \text{不被选用}\end{cases}$$

则该问题的数学表示为:

求目标函数的最大值: $\max \sum_{i=1}^{7} c_i x_i$,

$$\text{其中约束条件:}\begin{cases}x_1 + x_2 + x_3 \leqslant 2 \\ x_4 + x_5 \geqslant 1 \\ x_6 + x_7 \geqslant 1 \\ x_i = \{0,\ 1\}\ (i = 1,\ 2,\ \cdots,\ 7) \\ \sum_{i=1}^{7} b_i x_i \leqslant B\end{cases}$$

例 4 项目选择问题

某公司有机会对三个项目进行投资,根据该公司的预算,前两年每年能投资 6 万元,后两年每年能投资 7 万元,而这三个项目每年所需的投资额及利润如下表:

投资年度	项目所需投资额(万元)			投资额(万元)
	B_1	B_2	B_3	
第一年	0	4	2	6
第二年	5	1	2	6
第三年	4	2	3	7
第四年	5	2	3	7
利　润	17	10	16	

怎样选择投资项目可获得最大利润?

该公司对每个项目 $B_i(i = 1, 2, 3)$ 的投资仅有两种选择:投与不投,可用变量又 x_i 表示,并规定:

$$x_i = \begin{cases} 1 & \text{对 } B_i \text{ 投资} \\ 0 & \text{对 } B_i \text{ 不投资} \end{cases}$$

由于每年投资额的限制,故有

$$\text{约束条件:} \begin{cases} 4x_2 + 2x_3 \leqslant 6 \\ 5x_1 + x_2 + 2x_3 \leqslant 6 \\ 4x_1 + 2x_2 + 3x_3 \leqslant 7 \\ 5x_1 + 2x_2 + 3x_3 \leqslant 7 \\ x_i = \{0, 1\} \ (i = 1, 2, 3) \end{cases}$$

目标函数是利润 $L = 17x_1 + 10x_2 + 16x_3$,求使 L 最大的解是 $\{x_1, x_2, x_3\}$。

2. 0—1 规划的解法

上述 4 例都是规划问题,它们具有共同的特点:

1) 变量只能取 0 或 1;

2) 目标函数是变量的线性函数;

3) 约束条件也都是变量的线性函数。

这类规划问题称为 0—1 线性规划问题,简称 0—1 规划。0—1

规划反映的实际问题涉及面很广。

有 m 个变量的 0—1 规划，它的解至多有 2^m 个。如果变量数目不多，可列举出所有可能解，再检验它是否符合约束条件，然后从中选出最优解，这种方法称完全枚举法。如例 4 中共有 3 个变量，即 $m=3$，$x_i(i=1, 2, 3)$ 取 0 或 1，数组 (x_1, x_2, x_3) 有 2^3 个方案，分别为

$$(0,0,0),(1,0,0),(0,1,0),(0,1,1),$$
$$(1,1,0),(0,0,1),(1,0,1),(1,1,1)$$

先检查这些数组是否符合约束条件，其中满足约束条件的有六组：

$$(0,0,0)\quad L=0$$
$$(1,0,0)\quad L=17$$
$$(0,1,0)\quad L=10$$
$$(0,0,1)\quad L=16$$
$$(0,1,1)\quad L=26$$
$$(1,1,0)\quad L=27$$

比较这些解的优劣，使 L 最大的解是 $(1, 1, 0)$，即最优解为 $x_1=1$，$x_2=1$，$x_3=0$（投资 B_1、B_2 项目），此时 $L=27$。完全枚举法虽简单，但当变量较多时，计算十分麻烦，必须寻找适合多变量 0—1 规划的解法。

有一种专门用来解 0—1 规划的方法，称为匈牙利法，它是比较方便的。匈牙利法是通过一系列简约矩阵求得最优解，故也称为简约矩阵法。它是在匈牙利数学家库尼格证明了有关理论的基础上建立起来的。这种方法是通过对任务指派问题所给出的 $m\times m$ 阶矩阵进行一系列简化，使矩阵的每一行每一列都各含有一个"0"元素，然后根据这 m 个"0"元素（不唯一）即可得最优解。

以例 2 为例，题中的矩阵为

$$\begin{bmatrix} 3 & 14 & 10 & 5 \\ 10 & 4 & 12 & 10 \\ 9 & 14 & 15 & 13 \\ 7 & 8 & 11 & 9 \end{bmatrix}$$

将矩阵中第一行减去它的最小元素 3，该矩阵变换成：

$$\begin{bmatrix} 3-3 & 14-3 & 10-3 & 5-3 \\ 10 & 4 & 12 & 10 \\ 9 & 14 & 15 & 13 \\ 7 & 8 & 11 & 9 \end{bmatrix}$$

此时目标函数 T 变成 T'，变换后的目标函数为：

$$\begin{aligned} T' &= T - 3(x_{11} + x_{12} + x_{13} + x_{14}) \\ &= T - 3 \end{aligned}$$

（因为 $x_{11} + x_{12} + x_{13} + x_{14} = 1$）

显然，T'与原目标函数 T 仅差一个常数，T 与 T'能同时取最小（或最大）值，即 T 与 T'同解。因此，可以对矩阵的每行（或列）作加减变换，直到每一行每一列都含有"0"元素为止，都不会改变问题的最优解，只改变目标函数的值。例如，

$$\begin{bmatrix} 3 & 14 & 10 & 5 \\ 10 & 4 & 12 & 10 \\ 9 & 14 & 15 & 13 \\ 7 & 8 & 11 & 9 \end{bmatrix} \xrightarrow[\text{行的最小数}]{\text{每行减去本}} \begin{bmatrix} 0 & 11 & 7 & 2 \\ 6 & 0 & 8 & 6 \\ 0 & 5 & 6 & 4 \\ 0 & 1 & 4 & 2 \end{bmatrix} \xrightarrow[\text{4，第四列减 2}]{\text{第三列减去}} \begin{bmatrix} 0 & 11 & 3 & 0 \\ 6 & 0 & 4 & 4 \\ 0 & 5 & 2 & 2 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

最后这个矩阵的每一行每一列都含有"0"元素，矩阵经过这些变换后，只影响目标函数的值，而不会改变最优解。现在可按这个矩阵进行任务指派。为了使目标函数达到最小，可以从"0"元素最少的行开始指派，每行每列只指派一个"0"元素，指派到的"0"记为"0*"，同行同列的其他"0"元素不再指派，记为 Φ。由此可见，指派方式不是唯一的。按这种方法，前面的矩阵可变换为：

$$\begin{bmatrix} 0 & 11 & 3 & 0 \\ 6 & 0 & 4 & 4 \\ 0 & 5 & 2 & 2 \\ 0 & 1 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} \Phi & 11 & 3 & 0 \\ 6 & 0^* & 4 & 4 \\ 0^* & 5 & 2 & 2 \\ \Phi & 1 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} \Phi & 11 & 3 & 0 \\ 6 & 0^* & 4 & 4 \\ 0^* & 5 & 2 & 2 \\ \Phi & 1 & 0^* & \Phi \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} \Phi & 11 & 3 & 0^* \\ 6 & 0^* & 4 & 4 \\ 0^* & 5 & 2 & 2 \\ \Phi & 1 & 0^* & \Phi \end{bmatrix}$$

凡是“0”处的 $x_{ij}=1$，其他元素 $x_{ij}=0$，即指派结果为：

$$(x_{ij}) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

矩阵中 $x_{14}=1$，表示安排 A_1 做 B_4 工作；$x_{22}=1$，表示安排 A_2 做 B_2 工作；$x_{31}=1$，表示安排 A_3 做 B_1 工作；$x_{43}=1$，表示安排 A_4 做 B_3 工作。

在这种安排下，目标函数(总时间) T 为最小：

$$\begin{aligned} \min T = & 3\times0+14\times0+10\times0+5\times1 \\ & +10\times0+4\times1+12\times0+10\times0 \\ & +9\times1+14\times0+15\times0+13\times0 \\ & +7\times0+8\times0+11\times1+9\times0 \\ = & 5+4+9+11 \\ = & 29(\text{小时}) \end{aligned}$$

匈牙利算法比较方便，不需要特殊工具，仅靠纸与笔就可进行。当变量很多时，可通过计算机运算。现实世界中还存在着许多具有组合特征的、涉及“是”或“非”决策的最优化问题，这类问题也可归结为 0—1 规划。如果线性规划中的变量仅限于取整数时，这样的线性规划称为整数规划。显然，0—1 规划是整数规划的特殊情况。

3. 一般线性规划的问题

例5 某公司生产 A、B 两种产品，每种产品都需经过Ⅰ、Ⅱ两道工序加工。其中生产100件 A 产品需经Ⅰ工序加工7小时，Ⅱ工序加工4小时；生产100件 B 产品需经Ⅰ工序加工6小时，Ⅱ工序加工2小时。生产100件 A 产品可获利6万元，生产100件 B 产品可获利2万元。现在设备的条件限制是：Ⅰ工序的加工总工时不能超过43小时，Ⅱ工序的加工总工时不能超过16小时，问如何安排产品生产计划可使公司获利最多？

解　设安排生产 A 的产品数为 x（以百件计），安排生产 B 的产品数为 y（以百件计）。

据题意可得关系式：

$$\begin{cases} 7x+6y\leqslant 43 \\ 4x+2y\leqslant 16 \\ x\geqslant 0 \\ y\geqslant 0 \end{cases} \qquad ①$$

利润函数为

$$P(x,\ y)=6x+2y$$

本题所要解决的问题是：在满足条件①的 x、y 中，求出 x_0、y_0，使 $x=x_0$，$y=y_0$ 时，利润函数 $P(x,\ y)$ 达到最大值。

这里 $P(x,\ y)$ 也称为目标函数，①式中四个不等式称为对 x、y 的约束条件。

例6 某公司生产 A 和 B 两种饲料，每100单位 A 饲料的成本价值为11元，100单位 B 饲料的成本价值为8元。两种饲料含Ⅰ、Ⅱ、Ⅲ三种营养素。每100单位饲料所含各种营养素单位量如下：

	A 饲料	B 饲料
营养素Ⅰ	10	2
营养素Ⅱ	3	3
营养素Ⅲ	4	9

现在要求所生产的饲料中营养素Ⅰ的总含量至少要 20 单位，Ⅱ的总含量至少 18 单位，Ⅲ的总含量至少 36 单位。问：如何安排 A、B 两种饲料的生产量可以使总成本最少？

解　设安排生产 A 饲料 x(100 单位)，按排生产 B 饲料 y(100 单位)。

则根据题意可得约束条件：

$$\begin{cases} 10x + 2y \geqslant 20 \\ 3x + 3y \geqslant 18 \\ 4x + 9y \geqslant 36 \\ x \geqslant 0 \\ y \geqslant 0 \end{cases} \qquad ②$$

问题归结为约束条件②下，求 x 和 y 的数值，使目标函数(总成本) $G = 11x + 8y$ 达到最小值。

例 7　某工厂生产某种产品，需要在长度为 2 000 毫米的圆钢上截取长度分别为 600 毫米、750 毫米和 950 毫米三种规格的备用钢筋，这三种备用钢筋依次需要 100、200 和 300 根。怎样下料才能使余料最少？

解　采用搭配截取的方法。找出余料不足 600 毫米的一切下料方案如下表所示。

方案	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ
600	3	2	1	0	0	0
750	0	1	0	2	1	0
950	0	0	1	0	1	2
余料	200	50	450	500	300	100

设使用圆钢 x_i 根 ($i = 1, 2, \cdots, 6$)，按第 i 种方案下料。问题就归结为求 $x_1, x_2, x_3, \cdots, x_6$，满足约束条件

$$\begin{cases} 3x_1 + 2x_2 + x_3 \geqslant 100 \\ x_2 + 2x_4 + x_5 \geqslant 200 \\ x_3 + x_5 + 2x_6 \geqslant 300 \\ x_i \geqslant 0 \quad i = 1, 2, \cdots, 6 \end{cases}$$

使得余料

$$S = 200x_1 + 50x_2 + 450x_3 + 500x_4 + 300x_5 + 100x_6$$

为最少。

例 5、例 6、例 7 有下面三个特征：

1) 每个问题都要求一组未知数($x_1, x_2, \cdots, x_n$)，这组未知数的一组确定值就代表一个具体方案，通常要求这些未知数的取值都是非负的；

2) 存在一定的限制条件，称为约束条件。这些约束条件可用一组等式或不等式表示出来；

3) 都有一个目标要求，就是要求依赖于这组未知数的某个函数(称为目标函数)达到最大值或最小值。

如果约束条件和目标函数都是未知数的一次函数，则具有上述特征的问题称为线性规划问题。

4. 一般线性规划问题的解法

线性规划问题的解法不少，我们在此介绍两种。

(1) 线性规划问题的图解法

对于只含两个变量的线性规划问题可以用图解法求解。下面举例说明图解法。

用图解法求例 5 的解，求 x、y 满足约束条件：

$$\begin{cases} 7x + 6y \leqslant 43 \\ 4x + 2y \leqslant 16 \\ x, y \geqslant 0 \end{cases}$$

并使函数 $\max P(x, y) = 6x + 2y$ 达到最大值。

解　在以 x、y 为坐标的直角坐标系中，约束条件 $7x + 6y \leqslant 43$ 表示包含直线 $7x+6y=43$ 在内的左下半平面，约束条件 $4x + 2y \leqslant 16$ 表示包含直线 $4x+2y=16$ 在内的左下半平面。条件 $x \geqslant 0$, $y \geqslant 0$ 表示包含坐标轴在内的第一象限。如图 2.9.1，有阴影的凸多边形部分就是本线性规划问题的可行解域。

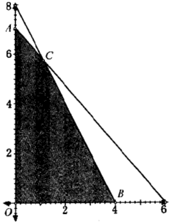


图 2.9.1

根据线性规划问题的理论可知，本题的最优解一定在凸多边形的四个顶点：O, A, C, B 中的某一个上取得。这四个顶点的坐标分别为

$$O(0,\ 0),\ A\left(0,\ \frac{43}{6}\right),\ C(1,\ 6),\ B(4,\ 0)$$

求出四个顶点上函数 $P(x, y)$ 的值并作比较，可求出其中最大者为 $P(4, 0) = 24$，即安排生产 A 产品 400 件、B 产品 0 件时获利最大，可获利 24 万元。

用图解法求例 6：

$$\begin{cases} 10x + 2y \geqslant 20 \\ 3x + 3y \geqslant 18 \\ 4x + 9y \geqslant 36 \\ x,\ y \geqslant 0 \end{cases}$$

求 $G(x, y) = 11x + 8y$ 的最小值。

仿例 5 的方法，可作出可行解域如图 2.9.2，它是一个含无穷远点的凸多边形，除了无穷远点外有四个顶点：

$$A(0,\ 10),\ B(1,\ 5),\ C\left(\frac{18}{5},\ \frac{12}{5}\right),\ D(9,\ 0)$$

在四个顶点上，$G(x, y)$ 的最小值为 $G(1, 5) = 51$。

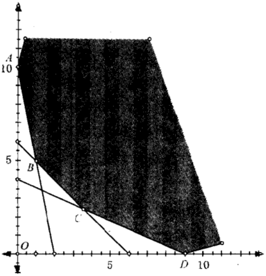


图 2.9.2

(2) 线性规划问题的单纯形解法

当一个线性规划问题的变量个数多于 3 时，图解法变成不可能，我们介绍另一种解法——单纯形解法。

为了叙述的方便，我们把如下问题称作是线性规划的标准型：

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \\ x_1 \geqslant 0,\ x_2 \geqslant 0,\ \cdots,\ x_n \geqslant 0 \end{cases} \qquad ③$$

$$b_1,\ b_2,\ \cdots,\ b_m \geqslant 0$$

求在约束条件③下目标函数

$$S = c_1x_1 + c_2x_2 + \cdots + c_nx_n$$

的最大值。

将非标准型的线性规划问题转化为标准型的方法是：

1) 若原来要求的是目标函数 S 的最小值，则只要令 $S_1 = -S$，

即变成求 S_1 的最大值问题了。

2) 若原来的约束条件为"$\leqslant$"的不等式,则只要在不等式左边加上一个新的非负变量即可使不等式变为等式。若原来的约束条件为"$\geqslant$"的不等式,则只要在不等式的左边减去一个新的非负变量,即可使不等式变为等式。所加上或减去的非负新变量称为松弛变量。松弛变量在目标函数中的系数可视为零。

3) 当某一约束方程的右端常数 b_i 为负数时,可在方程两端同时乘以(-1),使 $b_i \geqslant 0$。

我们用具体例子来说明单纯形法的计算方法和步骤。

例 8 设线性规划问题的约束条件为

$$\begin{cases} 6x_1 + 2x_2 \leqslant 180 \\ 4x_1 + 10x_2 \leqslant 400 \\ 3x_1 + 5x_2 \leqslant 210 \\ x_i \geqslant 0 \ (i = 1,\ 2) \end{cases}$$

求 $S = 31x_1 + 22x_2$ 的最大值。

解 先将这个线性规划问题化成标准型

$$\begin{cases} 6x_1 + 2x_2 + x_3 = 180 \\ 4x_1 + 10x_2 + x_4 = 400 \\ 3x_1 + 5x_2 + x_5 = 210 \\ x_1,\ x_2,\ x_3,\ x_4,\ x_5 \geqslant 0 \end{cases}$$

(其中 x_3、x_4、x_5 是松弛变量)

求 $S = 31x_1 + 22x_2$ 的最大值。

按问题所给的数据作以下单纯形表:

基变量		x_1	x_2	x_3	x_4	x_5	b	Q
I	x_3	6	2	1	0	0	180	30
	x_4	4	10	0	1	0	400	100
	x_5	3	5	0	0	1	210	70
	S	-31	-22	0	0	0	0	

作上述单纯形表的步骤是：

1) 上表的第 3—第 8 列是所给各方程中的系数和右端数值。第 5 行的数据由所给目标函数 $S = 31x_1 + 22x_2$ 中对应的系数确定。填写这一行数据时先将等式右端的各系数变号后填入相应的位置上。

在第 2 列(基变量列)前三行的位置上填写松弛变量，这三个位置称为基变量位置。接着考察 S 行上的数是否都是非负数。若无负数则计算到此结束，否则按下面 2)进行。

2) 在 S 行的负系数中选一个绝对值最大者(表中为 -31)。用该数所在列(表中是 x_1 列)上的数去除第 8 列(即 b 列)上相应的数，将商填入第 9 列(即 Q 列)相应的位置上。在所得商中求出最小数，这里 $\min\left(\frac{180}{6}, \frac{400}{4}, \frac{210}{3}\right) = 30$。

把 S 行上绝对值最大的数所在的列(表中是 x_1 列)与上述最小比值所在行上的数(表中是 6)称为主元。通常在它的右上角记"$*$"号。找出主元后，用主元所在列上的变量(表中是 x_1)去替换主元所在行上的变量(表中是 x_3)。被换出来的变量 x_3 用箭头"←"表出。然后用消去法化主元为 1，化主元所在的列的其他元素为 0。

3) 若 S 行上系数还有负数，则再重复 2)。可得主元 4，并用变量 x_2 去替换变量 x_5，再用消去法，使原主元所在位置为 1，它所在列的其他元素为 0。以上步骤重复进行，直至 S 所在行的系数全部非负为止。下表是本例的计算最优解的过程：

基变量		x_1	x_2	x_3	x_4	x_5	b	Q
I	$\leftarrow x_3$	6^*	2	1	0	0	180	30
	x_4	4	10	0	1	0	400	100
	x_5	3	5	0	0	1	210	70
	S	-31	-22	0	0	0	0	

(续表)

	基变量	x_1	x_2	x_3	x_4	x_5	b	Q
Ⅱ	x_1	1	$\frac{1}{3}$	$\frac{1}{6}$	0	0	30	90
	x_4	0	$\frac{26}{3}$	$-\frac{2}{3}$	1	0	280	32.3
	$\leftarrow x_5$	0	4^*	$-\frac{1}{2}$	0	1	120	30
	S	0	$-\frac{35}{3}$	$\frac{31}{6}$	0	0	930	
Ⅲ	x_1	1	0	$\frac{5}{24}$	0	$-\frac{1}{12}$	20	
	x_4	0	0	$\frac{5}{12}$	1	$-\frac{13}{6}$	20	
	x_2	0	1	$-\frac{1}{8}$	0	$\frac{1}{4}$	30	
	S			$\frac{89}{24}$	0	$\frac{35}{12}$	1 280	

由第 2 列出现的变量与最后第 2 列(即 b 列)对应的值可得,当 $x_1=20$, $x_2=30$, $x_4=20$ 时,S 的最大值为 1 280。

例 9 用单纯形法求解线性规划:

$$\begin{cases}-2x_1+x_2+3x_3\leqslant 2\\ 2x_1+3x_2+4x_3\leqslant 10\\ x_i\geqslant 0,\ i=1,\ 2,\ 3\end{cases}$$

求 $Z=x_1-2x_2+3x_3$ 的最小值。

解 令 $S=-Z$ 并引入松弛变量 x_4, x_5,将原问题化为标准形

$$\begin{cases}-2x_1+x_2+3x_3+x_4=2\\ 2x_1+3x_2+4x_3+x_5=10\\ x_i\geqslant 0,\ i=1,\ 2,\ \cdots,\ 5\end{cases}$$

求 $S=-x_1+2x_2-3x_3$ 的最大值。

用单纯形法求解,列表计算如下:

基变量		x_1	x_2	x_3	x_4	x_5	b	Q
Ⅰ	$\leftarrow x_4$	-2	1^*	3	1	0	2	2
	x_5	2	3	4	0	1	10	$\frac{10}{3}$
	S	1	-2	3			0	
Ⅱ	x_2	-2	1	3	1	0	2	
	$\leftarrow x_5$	8^*	0	-5	-3	1	4	$\frac{1}{2}$
	S	-3	0	9	2	0	4	
Ⅲ	x_2	0	1	$\frac{7}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	3	
	x_1	1	0	$-\frac{5}{8}$	$-\frac{3}{8}$	$\frac{1}{8}$	$\frac{1}{2}$	
	S	0	0	$\frac{57}{8}$	$\frac{7}{8}$	$\frac{3}{8}$	$\frac{11}{2}$	

由表可得 $x_1 = \frac{1}{2}$, $x_2 = 3$ 时,S 取得最大值$\frac{11}{2}$,从而 Z 取得最小值 $-\frac{11}{2}$。

单纯形法目前已有标准的计算机软件,使用时只需按要求输入目标函数和约束条件的具体数据,并运行这个软件,便可获得最优解。

习题

1. 用图解法求下列问题的解

$$\begin{cases} 9x_1 + 4x_2 \leqslant 360 \\ 4x_1 + 5x_2 \leqslant 200 \\ 3x_1 + 10x_2 \leqslant 300 \\ x_1, \ x_2 \geqslant 0 \end{cases}$$

求 $\max S = 7x_1 + 12x_3$。

2. 用单纯形法求解下列问题

$$\begin{cases} -2x_1 + x_2 + 3x_3 \leqslant 2 \\ 2x_1 + 3x_2 + 4x_3 \leqslant 10 \\ x_1,\ x_2,\ x_3 \geqslant 0 \end{cases}$$

求 $\max S = -x_1 + 2x_2 - 3x_3$。

第十节　选举中的数学

投票是民主政治的表现之一，可是很少有人知道数学和投票有着非常密切的联系。候选名额的分配，选举者选票的投法，判断当选的规定，党派联合的多数组成等等，一系列的问题都涉及数据的处理。因此，必要的数学知识已成为民主意识的组成部分。

1. 不同的选举方案

民主选举的最基本的原则是"多数选举"，即获得多数票的候选人当选；不过，投票的程序可以有很多种。假定候选人是 5 名，只有 1 人当选，常见的方案有：

① 简单多数票；

② 若无人过半数，则在两位获票最多的候选人之间增加一场决定性竞选；

③ 选举人可以对 5 名候选人中的一名投赞成票(+1)，对另一位不喜欢的人投反对票(−1)，最后以得票的代数和最高者当选(支持票数减去反对票数)；

④ 赞成选举法，对 5 名候选人中喜欢者都投票，选举者可以投 1—5 票，最高得票的一人当选；

⑤ 排序方案。选举人可以将 5 名候选人排队，即对 5 人中最满意的投 5 票，其次的投 4 票，再次的投 3 票，排第 4 位的只投 2 票，最不满意的投 1 票，不得弃权。

让我们来评论这 5 种方案。方案①优点是简单易行，缺点是当选者的得票数未必过半，还可能因为得票数第 2 和第 3 的人由于某

种原因而竞争特别激烈,使票数分散而落选,而实际能力不如他们俩的另一个人也许票数集中而当选。方案②较①为好,保证最后的当选者得票数过半,只是要选2次,比较麻烦。方案③允许投反对票,可以充分表达选举人的意愿,但是可能是缺点和优点都不突出的"中间人物"当选。方案④能够充分表达选民的倾向,使得当选者能够获得较多的选民拥护,不会出现选票分散的情形,缺点是实行比较困难,因为选举人有5票投票权,如何分配给这5个人有多种选择,没有投票经验的人往往会乱投一气,反而失去真实。方案⑤可能出现非常复杂的情况:人们共有20种不同的选择,容易失控。

例1 假设某团体打算外出旅游,有3个方向供选择:西湖,太湖,泰山。请21位成员投票决定。

可能有以下情况出现:

第一,按方案①,以简单多数确定。此时的票数为:西湖5票,太湖6票,泰山10票。结果泰山以10票中选。

第二,按方案②,令太湖和泰山对决。结果支持西湖的选票全部转向太湖,共11票,超过泰山的10票,于是太湖中选。

第三,按方案③,大家对去西湖不反对。5票赞成去西湖的人中有1人反对去泰山。但想到太湖的6人除了投太湖6张赞成票之外,因非常不愿爬山,对泰山投了6张反对票。而在愿意去泰山的10票中,对太湖投了7张反对票。这样,到太湖和泰山的人互相投了反对票,结果是:

$$\text{西湖}\quad 5-0=5(\text{票})$$

$$\text{太湖}\quad 6-7=-1(\text{票})$$

$$\text{泰山}\quad 10-6-1=3(\text{票})$$

于是,西湖中选,太湖竟然得了负票,不受欢迎。

第四,按方案④,每人可投1—3张选票。原投西湖的5人,也喜欢太湖,但不愿支持爬泰山,这组人的票数分布为5,5,0。

原投太湖的6人中,只投自己喜欢的太湖,不投其他的票。票数分布为0,6,0。

原喜欢泰山的10人中,7人反对去太湖,4人不反对游西游,甚至也赞成。这组人的票数分布为4, 3, 10。

现在的结果是:

西湖 $5+0+4=9$(票)

太湖 $5+6+3=14$(票)

泰山 $0+0+10=10$(票)

结果在方案③中最不受欢迎的太湖以14票当选。

第五,按方案⑤,这21个人对三个地方的喜欢程度可能出现如下情况:

5人选择 西湖得票数 > 太湖得票数 > 泰山得票数

6人选择 太湖得票数 > 西湖得票数 > 泰山得票数

10人选择 泰山得票数 > 西湖得票数 > 太湖得票数

于是,西湖票数 $3\times5+2\times6+2\times10=47$,

太湖票数 $2\times5+3\times6+1\times10=38$,

泰山票数 $1\times5+1\times6+3\times10=41$。

结果是在用方案①时最不受欢迎的西湖中选。

我们不妨让学生做些试验,例如,分别用这五种选举法在巩俐、潘虹、姜文、葛优、陈佩斯5个演员中选出一人为最佳影星。看看选举结果是否一致。

2. 代表的席位分配

选举课题的涉及面很广,简单的如代表席位的分配。美国宪法指出:"众议院议员的名额……将根据各州的人口比例分配。"但这么一句话,实行起来却问题不少。20多年来,关于"如何公正合理地分配席位"的争论,一直没有平息。

席位分配问题的数学描述是:

设众议院的议员席位数为 N,共有 s 个州,第 i 个州的人口数为

P_i，$i = 1, 2, \cdots, s$。问题是找一组数，$N_1, N_2, \cdots, N_s$，使得 $N_1 + N_2 + \cdots + N_s = N$，其中 N_i 表示第 i 州的议员席位数，并要求尽可能满足人口比例份额 Q_i，这里，

$$Q_i = \frac{NP_i}{P_1 + P_2 + \cdots + P_s}$$

最简单的方案是四舍五入法，即当 Q_i 不是整数时，小数部分按四舍五入法调整。但此时可能出现因四而舍去的州多，导致席位数空余，或者因五而入的州多，导致席位数不够。

1791 年，当时的美国的财政部长 A・哈密尔顿(Hamilton)提出的方案如下：

第一，先取各州人口份额 Q_i 的整数部分 $[Q_i]$；

第二，按 $R_i = Q_i - [Q_i]$ 的大小排列，将剩余的名额由 R_i 的大小顺序分配，分完为止。

这种方法似乎很合理，但有时也会产生令人费解的矛盾，请看下面的例题。

例 2 设学生代表会议按各系学生数比例分配代表名额。现有甲、乙、丙三系，各系的学生数依次是 100、60、40，代表总席位数为 20。此时，

$$N_1 = Q_1 = 10,\ N_2 = Q_2 = 6,\ N_3 = Q_3 = 4。$$

于是公平分配成功。

后来，各有 3 名学生分别从丙系转到甲系和乙系学习。于是

$$P_1 = 103,\ P_2 = 63,\ P_3 = 34$$

$$Q_1 = 10.3,\ Q_2 = 6.3,\ Q_3 = 3.4$$

$$R_1 = 0.3,\ R_2 = 0.3,\ R_3 = 0.4$$

按四舍五入法，将多出一个名额；按哈密顿方法，由于 R_3 为最大，则将剩余的一个名额给丙系，甲、乙、丙三个系的代表数分别是 10、6、4。难以理解的是，丙系学生数减少了 15%，但代表名额却没有变

化。甲、乙两系可能稍微会感到有些不公,但还是接受了。而后来发生的情况却让丙系难以接受了。

由于某种原因,学生代表会议的代表总数增加到 21 名。这时按哈密顿方法处理有如下结果:

系别	学生数	人数比例	按比例代表数	最终代表数
甲系	103	51.5%	10.815	11
乙系	63	31.5%	6.615	7
丙系	34	17%	3.570	3

这一结果自然引起丙系学生的不满。为什么代表席位总数增加一个,而分配给丙系名额反而减少一个?

此类状况在美国众议员的席位数分配上也曾经出现过。1880 年,美国阿拉巴马州对哈密顿方法提出异议,因为当议员总数增加时,该州议员席位反而减少。另外,当某州的人口增加率比其他州高时,议员数目也可能反而减少。人们感到哈密顿方法一定存在缺陷。

为了说明问题,请看下列关于 3 个席位的分配情况:

州别	人口数	按比例分配数	实际名额	人口增长率(%)	新人口数	新比例分配数	新实际分配数
甲	420	1.26	1	2.38	430	1.17	1
乙	455	1.365	1	14.39	520	1.42	2
丙	125	0.375	1	20	150	0.41	0
总和	1 000	3	3	10	1 100	3	3

按哈密顿方法,丙州的尾数0.375较乙州的尾数0.365和甲州的尾数 0.26 大,因此多获得一个名额。但当人口增加时,丙州的人口增加率最高,达到 20%,却因尾数 0.41 小于乙州的尾数 0.42,使乙州获得一个剩余名额,丙州却连一个代表也没有了。

这两个例子说明了哈密顿方法存在着"悖论",于 1910 年被废止在大选中应用。

从 1941 年起至今,美国国会分配名额采用的是亨丁顿方法。亨

丁顿(Huntington)是哈佛大学教授，20 世纪 20 年代提出用不公平程度概念来处理席位分配问题。

我们暂且讨论只有两方的情形。

已知 A 方和 B 方的人数分别为 p_A 和 p_B，得到的席位数分别为 n_A 和 n_B。

若 $\frac{p_A}{n_A}=\frac{p_B}{n_B}$，则该分配是公平的；

若 $\frac{p_A}{n_A}\neq\frac{p_B}{n_B}$，则该分配是不公平的。其中 $\frac{p_i}{n_i}(i=A, B)$ 较大的一方吃亏，即对这一方不公平。

在这种情况下，我们往往无法做到公平，因为如果得便宜的一方让出一席给吃亏的一方，又会使原先得便宜的一方变成吃亏的一方，仍然是不公平分配。为此我们要建立一项指标，来衡量不公平的程度。使得在不能公平分配的情况下，让我们做到不公平程度尽量小。

我们先想到一种简单的衡量方法：

设当 $\frac{p_A}{n_A}>\frac{p_B}{n_B}$ 时，用 $\frac{p_A}{n_A}-\frac{p_B}{n_B}$ 作为指标来衡量对 A 方的不公平程度。

例 3 设 A 方和 B 方各有人数 100 和 150，现有 6 个席位，他们的席位分配情况如下：

	A 方	B 方	总人数	不公平程度
人　数	100	150	250	
理论席位	2.4	3.6	6	
方案 1(对 A 不公平)	2	4	6	12.5
方案 2(对 B 不公平)	3	3	6	16.7

从表中可见，方案 2 的不公平程度较方案 1 大些，因此采用方案 1 更为合理些。

但是用指标 $\frac{p_A}{n_A}-\frac{p_B}{n_B}$ 来刻划不公平程度时也有缺陷，例如，当 $p_A=120,\ p_B=100,\ n_A=n_B=10$ 时，

$$\frac{p_A}{n_A}-\frac{p_B}{n_B}=12-10=2$$

当 $p_A=1\,020$, $p_B=1\,000$, $n_A=n_B=10$ 时,

$$\frac{p_A}{n_A}-\frac{p_B}{n_B}=102-100=2$$

常识告诉我们,后一种情况的不公平程度比前一种情况要好得多,但指标 $\frac{p_A}{n_A}-\frac{p_B}{n_B}$ 却反映不出来。因此有必要将该指标作改进,在 $\frac{p_A}{n_A}>\frac{p_B}{n_B}$ 时,规定用

$$r_A(n_A, n_B)=\frac{\frac{p_A}{n_A}-\frac{p_B}{n_B}}{\frac{p_B}{n_B}}$$

来刻划对 A 的不公平程度。

这时,前面讨论的问题中的不公平程度就可以有一个比较精确的刻划:在前一种情况中,对 A 方的不公平程度

$$r_A(10, 10)=\frac{\frac{120}{10}-\frac{100}{10}}{\frac{100}{10}}=0.2$$

在后一种情况中,对 A 方的不公平程度

$$r_A(10, 10)=\frac{\frac{1\,020}{10}-\frac{1\,000}{10}}{\frac{1\,000}{10}}=0.02$$

由于

$$r_A(n_A, n_B)=\frac{\frac{p_A}{n_A}-\frac{p_B}{n_B}}{\frac{p_B}{n_B}}$$

较准确地刻划了席位分配中的不公平程度,所以就能把握亨丁顿方法的基本原则——使分配中的不公平程度尽量小。这一方法还可推广到多方的席位分配问题中。

不过,亨丁顿方法仍有不足之处。到了1974年,两位美国人L·巴林斯基(Balinsky)和H. P. 杨(Young)提出了席位的公平分配公理:

公理1　人口增加不会失去席位。

公理2　平均说,每州应得到自己应分摊的席位。

公理3　总席位增加不会使某州的席位减少。

公理4　最后席位不会偏离比例份额。

公理5　从一个州到另一州的席位转让,不会使得这两个州都接近它们应得的份额。

1982年,巴林斯基和杨证明:不存在一个方案能满足以上五条公理。亨丁顿方法尽管还有毛病,但相比之下仍较为合理,所以现在还在使用。

3. 投票实力分析

西方国家实行多党制,在议会里各政党都有不同数额的席位。各政党未必可以单独取得多数而上台执政。因此,在没有一个政党获得绝对多数的情况下,几个政党联合组成多数联合执政的情况屡见不鲜。因此如何估计各党的投票实力,是一件颇为实用的事情。我国在政治上不搞多党制。但是在经济领域内,股份合作制中股票持有者的份额为多数时,将决定企业的发展前途,所以也是需要借鉴研究的。

让我们看一个实例。1972年,加拿大大选举行时的形势是:

自由党	109席
保守党	107席
新民主党	31席
其　他	17席
总　计	264席

超过 132 席为绝对多数。这时，只拥有 31 席的新民主党，与拥有 100 席以上的两个大党处于同样有利的地位。而“其他”的 17 席，在构成多数的联合中，处于“有你不多，无你不少”的无足轻重的位置。因此，一个政党在国会中拥有的席位数目固然重要，但是各党派席位形成格局同样需要研究。

设有 n 个政党，w_i 为第 i 个政党在国会中拥有的席位，全部席位数是

$$W = \sum_{i=1}^{n} w_i$$

用 S 表示 $\{N \mid N = 1, 2, \cdots, n\}$ 的一个子集，借助 S 描述若干个政党的联合。Q 是一个定额，表示执政党所需的最低票数，通常为 $W/2$ 或 $2W/3$。现在用 $[Q;\ w_1,\ w_2,\ \cdots,\ w_n]$ 表示 n 个政党分别具有 $w_1,\ w_2,\ \cdots,\ w_n$ 的一次竞争（政党可理解为股东，国会可理解为公司董事会）。

若有集合 S，使得

$$\sum_{i \in S} w_i > Q$$

则由 S 中各党派的联合可以执政。在股份公司的决策上，几个股东若联合持有公司 51%的份额，则有决策权。

例如：有 A、B、C、D 四股东，投票的格局为：

$$[Q;\ A,\ B,\ C,\ D]$$

分析以下几个模型：

模型Ⅰ　[51; 28, 24, 24, 24]

模型Ⅱ　[51; 25, 26, 26, 22]

模型Ⅲ　[51; 40, 25, 20, 15]

在模型Ⅰ中，A 的地位特别有利，B、C、D 处于同等地位；在模型Ⅱ中，A、B、C 之间有两者联合即可持有多数，彼此同等地位，D 虽然只比 A、B、C 少 3、4 票，却无足轻重；在模型Ⅲ中，A 仍据优势

地位，B、C、D 三派虽然票数有多有少，但作用却是一样的。

有些格局表面上不同，实质却是等价的。如[3; 2, 2, 1]，[8; 7, 5, 3]，[51; 49, 48, 3]，[2; 1, 1, 1]表示的格局没有本质区别。在[51; 49, 48, 3]中，3 票的小股东和 49 票的大股东，投票决策时具有同等的作用。

上面只是一种直观的观察。现在我们设法给出衡量某投票集团实力的数量化指标。

采用如上的记号。再用 P 表示 N 的所有可赢子集，即

$$P = \{S \subset N;\ \sum_{i \in S} w_i > Q\}$$

用 M 表示最小可赢联合(这一联合中再少任何一派便赢不到决定权)：

$$M = \{S \subset N;\ \sum_{i \in S} w_i > Q \text{ 且} \sum_{S \setminus i \in \{j\}} w_i < Q\}$$

对任何 $j \in S$。

对第 i 个竞争者(政党、股东、集团)，定义

$$M(i) = \{S \subset M;\ i \in S\}$$

用以表示 i 竞争者能够参与最小可赢联合全体，即找出在哪些可赢联合中少了 i 不行。于是我们定义 i 的实力

$$L(i) = \frac{1}{|M|} \sum_{S \in M(i)} \frac{1}{|S|}$$

这里$|M|$表示所有可赢联合体的数目，$|S|$表示 S 中元素个数。它反映了在所有可赢联合体中有多少个含 i 的最小可赢联合，而且考虑到在含 i 的最小可赢联合中是几家联合而成。

例如，有 A、B、C、D、E 五派竞争，格局为[5; 4, 2, 1, 1, 1]，则

$$M = \{AB、AC、AD、AE、BCDE\}$$

$$M(A) = \{AB、AC、AD、AE\}$$

于是 A 的实力为

$$L(A)=\frac{1}{5}\left(\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}\right)=\frac{2}{5}=\frac{8}{20}$$

由于

$$M(B)=\{AB、BCDE\}$$

于是 B 的实力为

$$L(B)=\frac{1}{5}\left(\frac{1}{2}+\frac{1}{4}\right)=\frac{3}{20}$$

同理 C、D、E 的实力为

$$L(C)=L(D)=L(E)=\frac{3}{20}$$

第三章

现代数学的若干进展

第一节 密码与编码

20 世纪的科学进步,向数学提出了新的课题。第二次世界大战时,英国及其同盟国的物理学家和电子工程师发明了雷达,雷达能准确地探测到德国战机的位置及其动向,为战胜希特勒法西斯发挥了巨大的作用。

大家知道,雷达的原理是发出电波束,碰到飞机时电波会反射回来,并为雷达所接收。显示屏上能够准确地显示出飞机的位置。但是,反射回来的电波强度很弱,而机器本身有许多噪声产生,散乱的噪声电波往往把我们所需要的反射电波淹没了。噪声,成为雷达设备发挥作用的主要障碍。从工程技术上考虑,总是尽量减少噪声、屏蔽噪声,同时加强发射功率,使得反射波的功率也能增强。这一切都有限度。发射功率大,噪声也跟着大,控制很难。

第二次世界大战结束之后,雷达成为民用航空、航天、航海等不可缺少的工具。这时,敏锐的数学家开始介入通讯中的噪声控制研究。1948 年,两项有关的成果公布于世。

第一项是 N · 维纳的《控制论》出版,这是数学控制论诞生的标志。在这项工作中,有一部分是"滤波",即将通讯中接收到的信息,滤去噪声,提取有用信息。当时苏联的大数学家柯尔莫哥洛夫(Kolmogorov 1906—1987)也独立地研究了滤波技术。

第二项成果也是在 1948 年,仙农从另一个角度保证信息准确传输:运用编码技术,使得收信人对接收到的信息,能够自动发现错误,并能改正错误。具体实现是在信息发送之前,就预先安排了可以自行监测错误发生的纠正码。这样,不必增加设备功率,只是用数学方法就提高了输送信息的效能。这是天才的设想,创新的构思。数学

家直接进入通信工程，直接产生经济效益，成为数学发展史上的又一辉煌的里程碑。这一节，我们将介绍编码与密码问题。

1. 能自动改正错误的编码技术

能自动改正错误的编码技术现在已广泛地用于日常生活之中。让我们看两个例子。

0 75070 31400 5

图 3.1.1

超市里用的条形码(也称 UPC 码)。在超市里，货物品种繁多。我们用一个 11 位数字的代码表示这个商品，如图 3.1.1。

超市的结算员用扫描器将代码输入电脑，代码将商品的产地、进货渠道、成本价、销售价格、现有库存量等等都标识得一清二楚，使用十分方便。但是，为了保证条形码的准确读取，准确记录，准确传送，需要复核。那么如何来检验“代码”是正确的呢？这就用了“检验码”。

请注意，图 3.1.1 中的条形码，共有 11 位数字 07507031400，后面跟着一个 5。这 11 位数字是条形码的本体。11 位数字可以代表 10^{11} 种不同的货物。实际上，一个超市里的货物品种至多 30 000 余种，远远用不完。最后的一个 5 是检验码。一般来说，如果条形码的数字依次是 a_{11}，a_{10}，$\cdots$，a_1，a_0，那么 a_0 要这样选取，使得

$$3a_{11}+a_{10}+3a_9+a_8+\cdots+3a_3+a_2+3a_1+a_0$$

恰是 10 的倍数。试检验图 3.1.1 中的条形码，将前 11 位数字代入公式，计算可得：

$$3\cdot 0+7+3\cdot 5+0+3\cdot 7+0+3\cdot 3+1+3\cdot 4+0+3\cdot 0=65$$

于是，a_0 就必须取 5，使得总数为 70。

这样编码，一旦条形码的 11 位数字有一个错了，或者某两个位置的数目颠倒了，用检验码 5 就可立即发现错误。要知道，这种错误

一旦发生，损失会很大。

我们还可以注意每本书后的国际统一书号 ISBN。我国出版的每一本书的封底上都印有这样的书号，见图 3.1.2。设 ISBN 的 9 个号码依次为 a_9，$a_8 \cdots a_1$，再加上最后一个号码 a_0，a_0 应确定为使得以下数目

$$10a_9 + 9a_8 + 8a_7 + \cdots + 2a_1 + a_0$$

是 11 的倍数。以图 3.1.2 的书号为例，我们得到前 9 项是

$$7 \times 10 + 5 \times 9 + 4 \times 8 + 3 \times 7 + 5 \times 6 + 2 \times 5 + 9 \times 4 + 7 \times 3 + 9 \times 2$$
$$= 70 + 45 + 32 + 21 + 30 + 10 + 36 + 21 + 18 = 283$$

再加上数值为 3 的 a_0，结果是 286，恰能被 11 除尽。

由上两个例子可见，编码技术已经影响到我们的日常生活。这种依靠人的聪明才智，不添加物质设备而得到经济效益的方法，是数学的特征。在当今的信息时代，我们看到了"数学技术可以直接产生经济效益"的又一佐证。

ISBN 7-5435-2979-3

9 787543 529793

图 3.1.2

下面让我们回到仙农的编码理论上来。在 1948 年的原始论文中，仙农引用了 R・汉明(Richard W. Hamming)发明的(7，4)码，说明如何设计一种可以发现错误并能改正错误的编码方案。众所周知，信息无非是一个 0 和 1 数字组成的序列，现在我们把要传送的由 0、1 组成的序列编组。每 4 个信息符号(0 或 1)加上另外 3 个检验符，构成一个由 7 位二进制数码组成的信息块，记之为：

$$x_1, x_2, x_3, x_4, x_5, x_6, x_7$$

其中 x_3，x_5，x_6，x_7 四个二进数码是要传递的信息，x_1，x_2，x_4 等 3 个是检验符。检验符选择的方法是：

x_4 要选择使 $a = x_4 + x_5 + x_6 + x_7$ 为偶数；

x_2 要选择使 $b = x_2 + x_3 + x_6 + x_7$ 为偶数；

x_1 要选得使 $c = x_1 + x_3 + x_5 + x_7$ 为偶数。

现在，假如我们接收到一组由 7 个二进数码组成的字母串，将它代入以上公式进行计算，如果 a、b、c 都是偶数，则表示传送正确，4 个信息数码确定无误。如果计算出的 a、b、c 有奇数，那就一定出错了。

仙农的这个设计，目的是要发现哪一个码是错的，以便加以改正。为此，要增加一个假设："传送的 7 个数码中至多可能出现一个错误"。在设备比较有效的情况下，这个假定不算苛刻。以下以 $a = 0$ 表示 a 为偶数，$a = 1$ 表示 a 为奇数，余同。

现在用接收到的 7 个数码计算 a、b、c 的奇偶，如果出错，可能发生 7 种情况（读者务必注意我们的假设——至多只有一个数码发生传送错误）：

$a = 1,\ b = 0,\ c = 0$	此时出现在 b、c 中的 x_5，x_6，x_7 都正确，因此错误出现在 x_4。
$a = 0,\ b = 1,\ c = 0$	同上，x_2 错。
$a = 0,\ b = 0,\ c = 1$	同上，x_1 错。
$a = 1,\ b = 1,\ c = 0$	此时出现在 c 中的 x_1，x_3，x_5，x_7 都对，a、b 表示式中的共同项是 x_6，故断定 x_6 错。
$a = 1,\ b = 0,\ c = 1$	同上，断定 x_5 错。
$a = 0,\ b = 1,\ c = 1$	同上，断定 x_3 错。
$a = 1,\ b = 1,\ c = 1$	因为 7 个数码只有一个是错的，而只有 x_7 在 a、b、c 的表示式中都出现，因此断定 x_7 错。

这样，使用(7，4)码的编码技术，在至多发生一个数码出错的情况下，我们不仅知道传送是否有错，而且可以知道那一个数码出错。这样的编码，成为具有自我纠错功能的编码。

数学，在这里确实是一种技术，一种可以直接用于通信的技术。编码只是通信的第一步，为了保持通信秘密，编制密码是又一项重要的技术。

2. 编 制 密 码

在商周时代,我们的祖先就会利用烽火传递军事信息。到北宋年间,军事学专家曾公亮发明了利用诗词来传递军事密件。在此以前,军事密件要派专人传送,不但费事,还会有送件人或有关人员离叛而失密的危险。曾公亮的方法是这样的:主帅给出征的大将军发一个密码本,其中将最常用的 40 个军事用语编好代码一一列出。

例如:

1) 请急增兵;

2) 请急增粮;

……

40) 贼军内讧,请派人离间。

主帅同时和将军约定一首五言律诗,这首诗的 40 个字要互不相同。例如下面的一首唐诗:

风劲角弓鸣,将军猎渭城。
草枯鹰眼疾,雪尽马蹄轻。
忽过新丰市,还归细柳营。
回看射雕处,千里暮云平。

将军在边疆需要写信时,先由所要报告的情况查得代码,再按次序在诗中找到对应的字。例如将军要报告的情况是“增粮”,代码是“2”,在上面诗中第 2 个字是“劲”,于是将军写一封无关紧要的信,信中要含有“劲”字。将军在“劲”字上作好记号,例如盖上印。在京城的主帅从“劲”字由诗及代码即可得知边疆要“增粮”。由于代码编排方法非常多,诗的选择也难以穷尽,敌人即使得到信件也是难以破译。

相比起来,更早的古罗马恺撒(公元前 100—公元前 44 年)使用过的另一种密码就要简单得多。这种密码现在称为恺撒码。恺撒码的编码方法是将文字中的每个字母向后移 3 位。为说明其方法,我

们用英语字母来作说明。

正规字母表和恺撒码对比表

正规字母	A	B	C	D	E	F	G	H	I	J	K	L	M
凯撒码	D	E	F	G	H	I	J	K	L	M	N	O	P
正规字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
凯撒码	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

例如下面一段文字(明文):

I CAME I SAW I CONQUERED("吾临吾睹吾胜"——恺撒名言),就变成下面一段密码:

L FDPH L VDZ L FRQTXHUHG

恺撒用这样的方法与他的将领通信,对写信的人和读信的人都很方便,而对局外人却有保密的作用。下面我们将介绍在编码中数学知识的一些应用。

(1) 余数的编码方法

我们用数学的观点来分析恺撒码的编码方法。其实,我们先规定数字 1—26 和 A—Z 的 26 个字母一种对应关系:

数字 1～26 与字母 A～Z 的对应表

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
数字	1	2	3	4	5	6	7	8	9	10	11	12	13
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
数字	14	15	16	17	18	19	20	21	22	23	24	25	26

恺撒码就是把正规的字母对应的数字加 3 后得到的新数字对应的字母。例如正规字母 D 对应的数字是 4,我们把它加 3,得到 7, 7 对应的字母是 G,因而 D 的恺撒码是 G。由于 24 以后的数加 3 后所得的和大于 26,而大于 26 的数字没有字母与之对应,此时我们将得到的和除以 26,再由所得的余数找对应的字母。这里我们规定,余数为 0 的字母对应 Z。这样我们把除以 26 后的各种余数与 26 个英语字母一一对应起来了。

现在我们用余数的方法讨论另一种形式的编码方法。

例 1 某旅店有 10 个房间，分别编以 1—10 个号码。设想我们要在每个房间的钥匙上刻上数字，刻的数字要使服务员很容易辨认是哪一个房间的钥匙，而使局外人不容易猜到。这也是一个编码问题。

我们可以在每把钥匙上刻上两个数字：第一位的数字是这把钥匙的房间号码除以 2 所得的余数；第二位的数字是这把钥匙的房间号码除以 5 所得的余数。我们把 1—10 十个数字和各种余数的情况一一对应了起来，得到如下密码：

房间号码和余数码的对应表

房间号码	1	2	3	4	5	6	7	8	9	10
钥匙密码	11	02	13	04	10	01	12	03	14	00

当服务员要开某个房间门的时候，按照密码的编制方法可以很快地根据房间的号码找到正确的钥匙。这就是说，由明码找密码是很容易的。现在我们来考虑一个相反的问题：如何由钥匙上的号码来确定是哪个房间的？即如何由密码来找到对应的明码。

我们先找两个基本数 a 和 b，它们有如下的性质：

a 被 2 除后余 1，即 a 是奇数；而 a 能被 5 除尽，即 a 是 5 的倍数。我们很容易得到，5 是 a 的一个解。

b 被 5 除后余 1，而能被 2 除尽，同样可以得到 6 是 b 的一个解。

如果一个钥匙上的号码为 MN，即第一位数字为 M，第二位数字为 N，我们先按下面的公式计算出数 c 来：

$$c = M \times a + N \times b$$

上述等式的右端第一项是能被 5 除尽的（这是由于 a 是 5 的倍数，因而第一项也是 5 的倍数），而由于 a 除以 2 后的余数为 1，因而第一项 $M \times a$ 除以 2 后的余数为 M；同样，右端第二项是能被 2 除尽的（这是由于 b 是 2 的倍数，因而这一项也是 2 的倍数），而由于 b 除

以 5 后的余数为 1，因而第二项 $N\times b$ 除以 5 后的余数为 N。因而数字 c 满足要求：

"除以 2 后余 M，除以 5 后余 N。"

由于 c 可能不在 1—10 的范围内，而我们讨论的房间号码只在 1—10 之间，于是可以取 c 除以 10 后的余数作为解。若除以 10 后的余数为 0，则对应第 10 号房间。

例如拿到的钥匙密码为 12，按上述公式计算 c：

$$c = 1\times 5 + 2\times 6 = 17$$

将 17 除以 10 后余 7，我们判断这是 7 号房间的钥匙。

(2) 用统计方法破译恺撒码

假设我们截获了敌方一份用密码书写的文件，并且知道是按恺撒码移位的方法编写的，但我们不知道密码是从明码移了几位得到的，我们如何破译这份密件？

最简单的方法是用尝试的方法，试用移一位、两位……的方法看看能否读懂密件的内容。如果我们会用计算机，这个尝试的工作可以由计算机来完成，否则要有极大的耐心。

除了尝试的方法，还可以采用统计的方法。其原理是：从大量的英语文字材料中统计各个字母应用的频率得知，26 个字母出现的频率很不相同的。下面就是一个统计结果：

26 个字母出现的频率表(%)

字母	A	B	C	D	E	F	G	H	I	J	K	L	M
频率	8	1	3	4	13	3	2	5	7	0	0	4	3
字母	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
频率	7	8	2	0	7	6	9	3	1	2	0	2	0

我们可以将密件中各个字母出现的频率按其次序一一列出，然后和上述表中的频率对照，以找出密码所移的位数。具体地可以这样做：将表中字母出现的频率依次序画出条形图如下(图 3.1.3)，这里画出了两个周期。

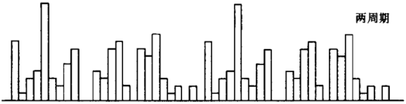


图 3.1.3

然后将密件上的各字母出现的频率条形图画在透明纸上(图 3.1.4)。将透明纸压在图上左右移动,找到两者比较相符的位置,就可以帮助我们确定密码所移的位数。

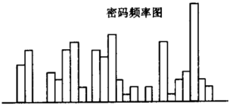


图 3.1.4

如果密码不是按照移位的方法,而是用一种一一对应的方法编制,即每个明码对应一个密码,不同的明码对应的密码也不同,则类似的统计方法也会有所帮助。

例如下面是一种一一对应密码表:

明码	A	B	C	D	E	F	G	H	I	J	K	L	M
密码	C	Q	F	E	P	U	J	K	O	L	N	D	H
明码	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
密码	Y	T	S	I	X	V	M	G	W	Z	A	B	H

我们会自然地想到,在敌人的密件中出现次数最多的字母多半对应明码字母 E(按上面的密码表可知这个密码字母是 P);出现次数多的其他字母可能对应明码 T、A、O、I、N、R,按上面的密码表,在密件中,它们依次以 M、C、T、O、Y、X 的身份出现。

这种方法虽然不能完全解决问题,特别是在密文材料较少的情况下,但是对破译密码总会有所帮助。

除了破译密码外，这种统计方法也可借鉴来解决其他问题。例如，要判断一篇文章的作者是两个作者中的哪一位（例如《红楼梦》的后四十回的作者究竟是曹雪芹还是高鹗）。由于一个作者使用的字、词、句通常有其偏爱，词和词之间的组合或搭配也会表现出一定的特点，我们首先设法找出这两个作者各自不同的特点。例如先从已经确认为这两个作者写的一些文章开始，对其中能反映作者特点的字、词、句出现频率作统计，并通过比较找出两人在各种字、词、句出现频率的差异。然后对要鉴定的文章中的这些字、词、句的出现频率也作出统计，将所得的频率和两位作者的频率对比，看看文章中这些字、词、句的频率和哪个人的特点接近。以此来帮助判断文章的作者。

(3) 利用矩阵编制更复杂的密码

从上面的叙述可以看到，一一对应的编码方法是比较容易被破译的。现在介绍一种借助矩阵来编制密码的方法，这类密码是很难破译的。

例 2 设有以下一句明码要传递：

MISSILE READY

按英语字母和数字的编码方法和下面几个常用的符号码：

符 号	空格	,	。	“
数 字	27	28	29	30

该明码的数字码应是：

13 9 19 19 9 12 5 27 18 5 1 4 25

假设我们用三位矩阵编码法来编制密码。先将上述明码按 3 位一组分组如下：

13 9 19|19 9 12|5 27 18|5 1 4|25 27 27|

这里我们在句子的最后加了两个空格，以凑足一组。

另外，我们选择一个矩阵作为编码阵。例如我们选下面的 A 作为编码阵：

$$A=\begin{pmatrix}0 & 1 & 2\\ 2 & -1 & 1\\ -1 & 1 & 0\end{pmatrix}$$

将第一组的明码(13 9 19)写成

$$\begin{pmatrix}13\\ 9\\ 19\end{pmatrix}$$

其密码由下面的公式求出：

$$A\begin{pmatrix}13\\ 9\\ 19\end{pmatrix}=\begin{pmatrix}0 & 1 & 2\\ 2 & -1 & 1\\ -1 & 1 & 0\end{pmatrix}\begin{pmatrix}13\\ 9\\ 19\end{pmatrix}=\begin{pmatrix}47\\ 36\\ -4\end{pmatrix}$$

即第一组的数字码(13　9　19)的密码为(47　36　−4)。同样可求出其他各组的密码。整句的密码序列为

$$47\ 36\ -4\ 33\ 41\ -10\ 63\ 1\ 22\ 9\ 13\ -4\ 81\ 50\ 2$$

为了解码,我们要由编码矩阵求出解码矩阵。我们把一组明码和它的密码分别记为

$$\begin{pmatrix}a\\ b\\ c\end{pmatrix}\quad 和\quad \begin{pmatrix}x\\ y\\ z\end{pmatrix}$$

因为明码和密码有下面的关系：

$$\begin{pmatrix}x\\ y\\ z\end{pmatrix}=\begin{pmatrix}0 & 1 & 2\\ 2 & -1 & 1\\ -1 & 1 & 0\end{pmatrix}\begin{pmatrix}a\\ b\\ c\end{pmatrix}$$

即有如下的关系式：

$$\begin{cases} b+2c=x,\\ 2a-b+c=y,\\ -a+b=z,\end{cases}$$

我们可以从上述方程组求出 a、b、c 由 x、y、z 表示的关系式：

$$\begin{cases} a = -x + 2y + 3z, \\ b = -x + 2y + 4z, \\ c = x - y - 2z。 \end{cases}$$

这里关系式的系数矩阵(即解码矩阵)为

$$B = \begin{pmatrix} -1 & 2 & 3 \\ -1 & 2 & 4 \\ 1 & -1 & -2 \end{pmatrix}$$

这样我们可以破译出密码 47 36 －4 的明码来：

$$\begin{pmatrix} -1 & 2 & 3 \\ -1 & 2 & 4 \\ 1 & -1 & -2 \end{pmatrix} \begin{pmatrix} 47 \\ 36 \\ -4 \end{pmatrix} = \begin{pmatrix} 13 \\ 19 \\ 9 \end{pmatrix}$$

注意，明码中两个相同的字母，译成密码后不一定相同。例如上述例子中，明码(MISSILE READY)中第 3、4 位上都是 S，但是相应密码中的第 3、4 位的数却不同：－4，33。这种编码方法显然要比一一对应的编码方法复杂得多。由于编码矩阵的选择有很大的自由度，确定几个明码为一组也可以各不相同，因此要破解这样的密码就困难得多。

3. 公开密钥体制

1976 年以后，Diffie 和 Hellman 提出公开密钥密码体制，使密码通讯揭开新的一页。本节将介绍它的数学背景。

公开密钥密码体制的基本思想是：每个通信者 X 有一加密的密钥 E_x 和一个解密的密钥 D_x；另一通信者 Y 也有 E_y、D_y，密钥 E_x、E_y、E_z……是公开的，像电话号码簿一样可以查，而解密密钥则是严格保密的。

明文用 P 表示，$E_x(P)$ 表示将 P 用 E_x 加密，即得到关于 X 的密

文 C_x。用数学式子写就是

$$E_x(P) = C_x,\ D_x(C_x) = P$$

即 $D_x \cdot E_x = I$。同理,对 Y 来说, $E_y(P) = C_y$, $D_y(C_y) = P$,即 $D_y \cdot E_y = I$ (I 表示恒等变换)。

如果第三者截取到一封密文,由于不知道消息的预定接收者是谁,更不知道接收者的解密密钥,因此要破译是非常难的。

为了介绍公开密钥体制,我们先来介绍所谓的"背包问题"。背包问题是一个数学问题,它是说一只背包最多能装 M 千克东西,一个人面对 n 件东西,每件重量为正整数 a_1, $a_2 \cdots a_n$,而 $\sum_{k=1}^{n} a_k > M$,试问能否从 n 件东西中选出若干件,使这些东西的总重量恰为 M,即背包内所装东西最多。从数学上说,这等于找一个二值数组 m_1, $m_2 \cdots m_n$,其中 m_k 只取 0 或 1,使

$$\sum_{k=1}^{n} m_k \cdot a_k = M$$

背包问题可能有解,也可能无解,虽然这一问题很简单,可是当 n 很大时,m_1, $m_2 \cdots m_n$ 的各种选法的数目极大(2^n 个),要确定是否有解,一般必须检查每种 m_1, $m_2 \cdots m_n$ 所取的值是否能使 $\sum_{k=1}^{n} m_k \cdot a_k$ 等于 M。2^n 是随 n 指数增长的,用最快的计算机去算也是比较困难的。

另一种是简单背包问题,是指 n 个正整数 a_1, $a_2 \cdots a_n$ 满足条件:

$$a_1 < a_2,\ a_1 + a_2 < a_3,\ \cdots,\ a_1 + a_2 + \cdots + a_{n-1} < a_n$$

简单背包问题有一个很快求解的方法如下:对于 M,先求适合 $a_{k_1} \leqslant M < a_{k_1+1}$ 的最大下标 k_1,再求适合条件 $a_{k_2} \leqslant M - a_{k_1} < a_{k_2+1}$ 的最大下标 k_2,如此继续,通过有限步之后,或者找到一个 k_i,使得 $a_{k_i} = M - a_{k_1} - a_{k_2} - \cdots - a_{k_i-1}$,或者没有这样的 k_i。若是前者,问

题有解，$m_{k_1} = m_{k_2} = \cdots = m_{k_i} = 1$，其余 $m_k = 0$，这就找到了解 $(m_1, m_2, \cdots, m_n)$，若是后者，则问题无解。

例 3 设 $a_1 = 1, a_2 = 3, a_3 = 5, a_4 = 10, a_5 = 21$。则五个数可构成简单背包问题。试问当 $M = 16$ 时，此问题是否有解？

因为 $a_4 = 10, a_5 = 21$，此时 $a_4 < M < a_5$，$M - a_4 = 6$，又有 $a_3 < M - a_4 < a_4$，$M - a_4 - a_3 = 1$，$a_1 \leqslant M - a_4 - a_3 < a_2$。因而 $M = a_1 + a_3 + a_4$，于是问题有解$(1, 0, 1, 1, 0)$。

此问题当 $M = 17$ 时无解。

上述例题中数字较少，可用笔算凭直观算出，当 n 较大时笔算的困难会大些，但计算步骤最多不超过 n 步，还是可以算的。但用计算机则会更快些。

现在回到公开密钥密码体制。设通信的明文是一个长度为 n 的二元数组（即不是英文字母，而是已经翻译成只取 0 或 1 的二进制数码序列），这个 n 一般是很大的，少则上百，多则上万。大多是可以分段处理，以公开密钥的长度为单位分段拍发。我们记为

$$P = (p_1, p_2 \cdots p_n),\ p_i = 0 \text{ 或 } 1$$

由于简单背包问题易解，我们取 $B = (b_1, b_2, \cdots, b_n)$ 为一个简单背包。现在设法从 B 中做出一个非简单背包 $A = (a_1, a_2 \cdots a_n)$ 作为公开密钥。其做法是，先选取两个整数(w, u)作为密钥参数（这两个参数自己选定以后是严格保密的），使

$$u > \sum_{i=1}^{n} b_i,\ w < u,\ (w, u) = 1$$

然后令

$$a_i \equiv wb_i (\operatorname{mod} u),\ i = 1, 2 \cdots n$$

$(a_1, a_2 \cdots a_n)$是个普通的背包，这样一个背包体制就完成了。现在描述一下通信过程。

设 X 发送信息 P 给 Y，$P = (p_1, p_2 \cdots p_n)$。

第一步 X 用 Y 的公开加密密钥 $E_Y = (a_1, a_2 \cdots a_n)$ 进行加密，

密文 C 是 $\sum_{i=1}^{n} p_i a_i$，这是一个正整数；

第二步　X 将 C 发给 Y；

第三步　Y 收到 C 后，用 (w, u) 从 C 求出简单背包 $(b_1, b_2 \cdots b_n)$，再解此问题，得出二元数组 $(p_1, p_2 \cdots p_n)$，即原来的明文。其数学原理为：

$$C \equiv \sum_{i=1}^{n} p_i a_i \equiv \sum_{i=1}^{n} p_i w b_i \equiv w \sum_{i=1}^{n} p_i b_i \pmod u$$

故
$$w^{-1} C \equiv \sum_{i=1}^{n} p_i b_i \pmod u$$

因此，Y 收到 C，即可以用自己知道的 (w, u) 算得

$$w^{-1} C \equiv b_i \pmod u, \ i = 1, 2 \cdots n$$

由于 w, u 和 $(a_1, a_2 \cdots a_n)$ 都是 Y 知道的，所以计算 b_i 是很容易的。最后对 $(b_1, b_2 \cdots b_n)$ 和 $w^{-1}C$ 这个简单背包问题求解，得出的 $(p_1, p_2 \cdots p_n)$ 即为明文。

例 4　Y 对简单背包 $B = (1, 3, 5, 10, 21)$ 取 $w = 7$, $u = 45$（将 B 和 w, u 保密）。因为

$$7 \equiv 7 \times 1 \pmod{45}$$

$$21 \equiv 7 \times 3 \pmod{45}$$

$$35 \equiv 7 \times 5 \pmod{45}$$

$$25 \equiv 7 \times 10 \pmod{45}$$

$$12 \equiv 7 \times 21 \pmod{45}$$

$$1 \equiv 7 \times 13 \pmod{45}$$

故取 $A = (7, 21, 35, 25, 12)$, $w^{-1} \equiv 13 \pmod{45}$。

Y 将 A 公开在密钥表上。X 从表上查知 Y 的公开密钥 A。现在 X 要送信息 $P = (1, 1, 0, 1, 0)$ 送给 Y，用 A 将 P 加密，即得

$$C = \sum_{i=1}^{5} p_i a_i = 7 + 21 + 25 = 53$$

X 将 53 发给 Y，Y 收到后先算

$$w^{-1}C \equiv 13 \times 53 \equiv 14 \pmod{45}$$

Y 只需对 $M = 14$ 求简单背包 $B = (1, 3, 5, 10, 21)$ 的解，即可知原文为 $P = (1, 1, 0, 1, 0)$。

习题

1. 将下面一句英语译成恺撒码。

(1) *WHAT TIME IS IT*

(2) *IT IS RAINING NOW*

(3) *CALL THE POLICE*

2. 破译下面一段用恺撒码写成的密文。

(1) *VNB LV EOXH*

(2) *KDLO FDHVDU*

(3) *L KDYH D KHDGDFKH*

3. 试用 3 和 5 两个数字对十个房间的钥匙编制密码。这时由钥匙密码如何求出房间号码？试以密码为 23 的钥匙加以说明。

4. 如果我们要同时对 100 个房间的钥匙编制密码，仿照余数法应该如何做？用 3、5、7 三个数字编制一个三位的密码试试看。

5. 仔细观察在计算机键盘上各字母的位置，遵照标准指法，那些最常用的字母是归哪几个手指击打的？想想和这些手指的灵活性有什么关系。

6. 用本节中的编码矩阵，把下面的句子先变成数字码，再译成密码。

(1) *SO FAR SO GOOD*

(2) *HELP*

7. 用本节中的解码矩阵，破译下面的密码。

(1) 20 23 −2 31 15 5 72 19 13

(2) 74 9 19 45 28 1 72 28 10

8. 用编码阵

$$\begin{pmatrix} 4 & -7 \\ -1 & 2 \end{pmatrix}$$

把下面的句子译成密码：

PROFESSOR HAS GONE

9. 利用所求出的解码阵，破解下面一段密文：

53 32 3 15 60 −26 54 16 9

10. 请甲、乙两位学生配合，实施一次公开密钥的密码通讯。

第二节　如虎添翼的迭代方法

随着20世纪40年代电子计算机的出现和飞速发展，在各门自然科学和工程、科学技术的发展中，“科学计算”已经成为平行于理论分析和科学实验的第三种手段。而“算法数学”（也称数值计算或数值分析）又是科学计算过程中不可缺少的重要环节。无论是在高科技领域还是传统的学科领域，算法数学都有着广泛的应用。在创造性工作的先行性研究中更具有突出的作用。

1. 算法研究的意义

算法数学的研究对象主要是那些通过计算机来求得数学问题的数值近似解的方法和过程。例如对于一个实际问题，先把它归结为数值算法问题，即由一组已知数据（又称输入数据），求出一组结果数据（又称输出数据），使得这两组数据之间，满足预先指定的某种关系。对数值问题的输入数据进行处理，判断此数值问题是否有解；在解存在的情况下，给出输出数据，这种过程称为算法。当解不存在时，算法应能作出明确的判断，最好能指出解不存在的关键。对于每一种数学问题的近似解法，算法数学不仅要讲明它的基本原理，给出计算公式，还必须研究它的具体实施（算法）以及近似解与精确解之间的近似程度。

研究算法的意义归纳起来有下面几点。

(1) 构造计算机能用的算法

由于计算机基本上只会做加、减、乘、除四则运算和逻辑运算，所以将数学问题转化为算法时必须化为计算机能执行的运算。此外，

如果在科技和工程中提出的数学问题必须通过无限次运算才能得到精确解，那么需设法构造只能采用有限步得其近似解的算法。

(2) 怎样计算才能既快又省

虽然计算机有很高的运算速度和大量的信息存贮单元，但在计算大型课题时仍时常感到花费机时太多与存贮单元紧张。因此设计算法时应尽量减少运算量，节约存贮单元。

(3) 怎样计算才可靠

由于在计算机上数的表示只能是有限位，所以无理数和数位较长的有理数只能按舍入原则化为机器允许的有限位才能参与计算。不同的计算方案对舍入误差的敏感程度不同。如果一个算法的计算结果受舍入误差的影响较小，则称这算法是数值稳定的。否则称为数值不稳定的。设计的算法应尽量做到数值稳定。

总之，我们研究算法，就是要寻求一个运算量小、存贮量小、逻辑结构简单、且具有数值稳定性好的算法。

下面我们着重介绍两类迭代算法。

2. 迭代法的基本思想

所谓迭代，可看作同一个运算或操作的多次重复。自然数的乘法 $a \times k$，即 k 个 a 的累加

$$\underbrace{a + a + \cdots + a}_{k}$$

可看作加法运算或函数 $f(x) = x + a$ 的迭代。同样，乘方也可以理解为迭代。我们熟悉的等差数列和等比数列的计算公式显然也是迭代产生的。迭代是自然科学乃至人类生活的一个常用方法。在实践中，我们常常通过对初始状态到当前状态的记录，来分析系统运动的规律。有时，从一个状态到下一个状态的变化遵从同一个规则，这一规则一旦被发现，我们就可以确定和预测系统的演变，这就是所谓确定性系统的思想，实质上是一种迭代思想。

例如生态学中研究的昆虫种群量模式

$$x_{n+1} = x_n(a - bx_n),\ 0 \leqslant x_n \leqslant \frac{a}{b}$$

可看作函数 $f(x) = x(a - bx)$ 的迭代。

又如,X-射线的透射可看作射线衰减率的迭代;在流体渗流,传热和其他动力学模型中,还可以举出许多迭代的例子。

在数学和计算机科学研究中,常常用数值方法把微分方程化为迭代,以便设计计算程序。还常常通过相空间上庞加莱映射的迭代,来分析向量的周期性和混沌性。在经济生活中,我们时常计算存款和贷款的本利和,如果本金 p 以年利率 r 借贷 n 年,按单利结算,其总和为

$$A_n = p(1 + nr)$$

若按复利结算,其总和为

$$A_n = p(1 + r)^n$$

显然,A_n 分别是函数

$$a(x) = x + rp \text{ 和 } a(x) = x(1 + r)$$

的迭代。

我们先来看一个来自日常生活中的函数迭代问题。

例 1 一个容积为 0.5 升的杯子盛满沏好的茶水,按通常喝水的习惯:喝掉$\frac{2}{3}$后再加满开水,加 5 次水后认为是喝淡了。如果能测定此时茶质和水的比例为 a,问最初的茶水比是多少?

设最初的茶水比是 x,则喝完一次并加满水后的茶水比是

$$f(x) = \frac{x}{2x + 3}$$

于是问题化为:已知 f 的 5 次迭代 $f^5(x) = a$, 求 x。

可直接计算得

$$f^2(x)=f(f(x))=f\left(\frac{x}{2x+3}\right)=\frac{\frac{x}{2x+3}}{\frac{2x}{2x+3}+3}$$

$$=\frac{x}{8x+9}=\frac{x}{(3^2-1)x+3^2}$$

类似可求出 $f^3(x)$, $f^4(x)$, $f^5(x)$,而

$$f^5(x)=\frac{x}{(3^5-1)x+3^5}$$

由 $f^5(x)=a$ 易解得

$$x=\frac{3^5\cdot a}{1-(3^{10}-1)a}$$

由此可见,计算 f 的 5 次迭代法是解决这一问题的关键。

计算函数的迭代不仅重要而且有趣。对给定的函数,我们希望计算其迭代的表达式,尤其是一般的 n 次迭代法。例如:

若 $f(x)=x+b$,则 $f^n(x)=x+nb$;

若 $f(x)=cx$,则 $f^n(x)=c^nx$;

若 $f(x)=x^k$,则 $f^n(x)=x^{k^n}$。

对于稍微复杂一点的初等函数,我们有两种常用方法。

3. 不 动 点 法

定义 1 若 $x_0\in D$, $f(x_0)=x_0$, 则称 x_0 为 f 的不动点。

如果能断定一个函数 f 的迭代式的基本代数形式,如线性式,线性分式,多项式等,我们可以设置待定常数,并且用函数 f 的不动点来确定这些常数。

例 2 已知 $f(x)=ax+b$, a, $b\in\mathbf{R}$, $a\neq1$, 因为 $f(x)$是线性函数,所以 $f^n(x)$也是线性函数,不妨设

$$f^n(x)=a^nx+B$$

其中 B 待定。从 $f(x)=x$ 解出 f 的不动点 $x_0=\frac{b}{1-a}$，由 $f(x_0)=x_0$，必然有 $f^n(x_0)=x_0$，这一关系表明

$$a^n\cdot\frac{b}{1-a}+B=\frac{b}{1-a}$$

从中解出

$$B=\frac{1-a^n}{1-a}\cdot b$$

从而

$$f^n(x)=a^n x+\frac{1-a^n}{1-a}\cdot b$$

4. 共轭相似法

定义 2 如果存在可逆函数 $h(x)$，使函数 f 与 g 满足

$$f=h^{-1}\circ g\circ h$$

（其中 $y=f\circ g(x)$ 表示复合函数 $y=f(g(x))$）。
就称 f 与 g 共轭或相似，记为 $f\sim g$。

共轭是一种等价关系，即满足自反性、对称性、传递性。

因为由 $f=h^{-1}\circ g\circ h$，可以推导出 $f^n=h^{-1}\circ g^n\circ h$，所以 $f\sim g\Rightarrow f^n\sim g^n$。我们常用这个性质，把一个复杂的函数迭代化为一个较简单的函数迭代，此种方法关键在于找 $h(x)$，$g(x)$。

考虑例 2，取 $h(x)=x+\frac{b}{a-1}$，求出 $h^{-1}(x)=x-\frac{b}{a-1}$，令 $g(x)=a$，则

$$f(x)=h^{-1}(ah(x))=a\left(x+\frac{b}{a-1}\right)-\frac{b}{a-1}$$

从而 $$f^n(x)=h^{-1}(a^n h(x))=a^n\left(x+\frac{b}{a-1}\right)-\frac{b}{a-1}$$

$$= a^n x + \frac{a^n - 1}{a - 1} \cdot b$$

同样得到上述结果。

例 3 已知有理函数

$$f(x) = \frac{ax + b}{x + c}$$

其中 $a, b, c \in \mathbf{R}$, $ac - b \neq 0$, 则有

$$f^n(x) = s + \frac{(a-s)^n (x-s)}{((a-s)^n - (s+c)^n) x_0 (x-s) + (s+c)^n}$$

其中 s 是二次方程 $s^2 - (a-c)s - b = 0$ 的根, $x_0 = \frac{1}{a-c-2s}$。

事实上,令 $h(x) = \frac{1}{x-s}$,则有 $h^{-1} = \frac{1}{x} + s$, 由 s 的定义知它是 f 的一个不动点,从而

$$f(h^{-1}(x)) = \frac{a + asx + bx}{1 + sx + cx} = \frac{a-s}{1+(s+c)x} + s$$

进而

$$h(f(h^{-1}(x))) = \frac{1}{f(h^{-1}(x)) - s} = \frac{1+(s+c)x}{a-s}$$

$$= \left(\frac{s+c}{a-s}\right)x + \frac{1}{a-s}$$

再令

$$g(x) = \left(\frac{s+c}{a-s}\right)x + \frac{1}{a-s}$$

此时 g 是一个线性函数。从而建立了共轭关系

$$h(f(h^{-1}(x))) = g(x)$$

由 g 的线性形式可算出

$$g^n(x) = \left(\frac{s+c}{a-s}\right)^n x + \frac{1}{a-s}\sum_{k=0}^{n-1}\left(\frac{s+c}{a-s}\right)^k$$

$$= \left(\frac{s+c}{a-s}\right)^n x + \frac{1}{a-s}\,\frac{\left(\frac{s+c}{a-s}\right)^n - 1}{\frac{s+c}{a-s} - 1}$$

$$= \left(\frac{s+c}{a-s}\right)^n (x - x_0) + x_0$$

这里 $x_0 = \frac{1}{a-c-2s}$。于是

$$f^n(x) = h^{-1}(g^n(h(x))) = \left(g^n\left(\frac{1}{x-s}\right)\right)^{-1} + s$$

$$= s + \frac{(a-s)^n(x-s)}{((a-s)^n - (s+c)^n)x_0(x-s) + (s+c)^n}$$

从而证实了结论。

有些看来复杂的函数,其迭代其实很简单。

例 4 对于 $f(x) = \frac{x}{\sqrt[k]{1+ax^k}}$

令 $$h(x) = x^k,\ g(x) = \frac{x}{1+ax}$$

易见,$f(x) = h^{-1}(g(h(x)))$ 直接计算或利用例 3 的结果,知

$$g^n(x) = \frac{x}{1+nax}$$

从而 $$f^n(x) = \frac{x}{\sqrt[k]{1+nax^k}}$$

上述例子中,我们常常用共轭相似法把函数化成 $g(x) = cx$ 或 $g(x) = x+b$ 形式。这是典型的哈特曼一格诺曼线性化思想。要确定共轭变换 $h(x)$,就要解函数方程

$$h(f(x)) = ch(x) \text{ 或 } h(f(x)) = h(x)c$$

这正是著名的施罗德方程和阿贝尔方程。除了对一些特殊类型的函数外，无论用什么方法求解迭代式，都是一件困难的事。也就是讲，有限迭代法除了对函数的类型有特殊要求外，技巧性也特别强。对一般的函数方程，我们就必须引进无限迭代的思想，这在下节中讨论。

5. 迭代法求方程的根

迭代法是一种逐次逼近法。它是求解代数方程，超越方程及方程组的一种基本方法，但存在收敛性及收敛速度问题。

为了用迭代法求非线性方程 $f(x)=0$ 的近似根，首先需要将方程 $f(x)=0$ 转化为等价方程

$$x=g(x)$$

显然，将 $f(x)=0$ 转化为形如 $x=g(x)$ 的等价方程的方法有很多种。

例 5 方程 $f(x)=x-\sin x-0.5=0$ 可转化为以下两种不同形式的等价方程：

1) $x=\sin x+0.5\equiv g_1(x)$；

2) $x=\sin^{-1}(x-0.5)\equiv g_2(x)$。

定义 3 设方程为 $x=g(x)$，选取一个方程的初始近似解 x_0，且按下述逐次代入法，构造一近似解序列：

$$\begin{cases} x_1=g(x_0) \\ x_2=g(x_1) \\ \vdots \\ x_{k+1}=g(x_k) \\ \vdots \end{cases}$$

这种方法称为迭代法。$g(x)$称为迭代函数。

如果由迭代法产生的序列$\{x_k\}$有极限存在，即 $\lim\limits_{k\to\infty} x_k=x^*$，称

$\{x_k\}$为收敛或称迭代过程收敛。否则称$\{x_k\}$不收敛。

设 $g(x)$为连续函数,且 $\lim\limits_{k\to\infty} x_k = x^*$,则有

$$x^* = \lim_{k\to\infty} x_{k+1} = \lim_{k\to\infty} g(x_k) = g(\lim_{k\to\infty} x_k) = g(x^*)$$

由于 $x^* = g(x^*)$,故 x^* 是方程 $x = g(x)$ 的解,自然也是方程 $f(x) = 0$ 的解。

显然,在由方程 $f(x) = 0$ 转化为等价的方程 $x = g(x)$ 时,选择不同的迭代函数 $g(x)$,就会产生不同的序列$\{x_k\}$,(即使初始值 x_0 选值一样),且这些序列的收敛情况也不会相同。

例 6 对例 5 中的方程,用迭代法求根。

1) $x_{k+1} = \sin x_k + 0.5$, $(k = 0, 1, 2 \cdots)$

2) $x_{k+1} = \sin^{-1}(x_k - 0.5)$, $(k = 0, 1, 2 \cdots)$

k	x_k	
	(a)	(b)
0	1.0	1.0
1	1.341 471	0.523 599
2	1.473 820	0.023 601
3	1.495 301	−0.496 555
4	1.497 152	−1.487 761
5	1.497 289	无意义
6	1.497 300	无意义
7	1.497 300	无意义

由上表中的计算结果可看出,我们选取的两个迭代函数分别构造的迭代序列$\{x_k\}$收敛情况不一样(初始值都取为 1.0),在 1)情况下$\{x_k\}$收敛,并且 $x^* \approx 1.497\,300$;而在 2)情况下,出现计算式无定义。所以用迭代法求方程 $f(x) = 0$ 的近似根时,必须注意迭代函数 $g(x)$的选取,以确保迭代过程 $x_{k+1} = g(x_k)$ 的收敛。

下面将介绍判定迭代过程是否收敛的若干定理。

定理 1 设有方程 $x = g(x)$ 满足

1) 当 $x \in [a, b]$ 时，$g(x) \in [a, b]$；

2) 存在正数 $L < 1$，使对任意 $x \in [a, b]$，有

$$|g'(x)| \leqslant L$$

则 1) 方程 $x = g(x)$ 在 $[a, b]$ 上有唯一的根 x^*；

2) 对任意初始值 $x_0 \in [a, b]$，迭代公式

$$x_{k+1} = g(x_k),\ k = 0,\ 1,\ 2,\ \cdots$$

收敛。且 $\{x_k\}$ 收敛于 x^*；

3) 有误差估计式

$$|x^* - x_k| \leqslant \frac{L}{1-L}|x_k - x_{k-1}|$$

$$|x^* - x_k| \leqslant \frac{L^k}{1-L}|x_k - x_0|$$

例 7 试用迭代法求方程 $f(x) = x - \ln(x+2) = 0$ 在 $[0, 2]$ 内的根。

解 将原方程化为等价方程：

$$x = \ln(x+2) = g(x)$$

由于 $g(0) = \ln 2 \approx 0.6931 > 0$，$g(2) = \ln 4 \approx 1.386 < 2$，且 $g(x)$ 为增函数，故当 $0 \leqslant x \leqslant 2$ 时，$0 \leqslant g(x) \leqslant 2$，又由

$$g'(x) = \frac{1}{x+2}$$

则当 $x \in [0, 2]$ 时，有

$$|g'(x)| = \frac{1}{x+2} \leqslant g'(0) = \frac{1}{2} < 1$$

于是由定理 1 可知，当初值 $x_0 \in [0, 2]$ 时，迭代过程 $x_{k+1} = g(x_k)$ 收敛。

如果要求 x^* 的近似解，准确到小数点后第 6 位，即要求

$$|x^* - x_k| \leqslant \frac{1}{2} \times 10^{-6}$$

计算过程列表如下：取 $x_0 = 0$

k	x_k
0	0
1	0.693 147 18
2	0.990 710 46
⋮	⋮
14	1.146 193 1
15	1.146 193 2

由表可知 $|x_{15} - x_{14}| \approx 10^{-7}$，且 $L = \frac{1}{2}$，故

$$|x^* - x_{14}| \leqslant \frac{1}{1-\frac{1}{2}} |x_{15} - x_{14}|$$

$$\approx 2 \times 10^{-7} < \frac{1}{2} \times 10^{-6}$$

所以 $x^* \approx 1.146\ 193\ 1$，$|f(x_{14})| \approx 0.8 \times 10^{-7}$。

定理 1 的条件一般不易验证，对于大范围的含根区间，定理 1 的条件也不一定成立。其实，在实际应用迭代法时，总是在根 x^* 的邻近考察，这就是所谓的局部收敛性。

定义 3 如果在 x^* 的某个邻域 S：$|x - x^*| < \delta$ 内，对于任意初始值 $x_0 \in S$，迭代过程 $x_{k+1} = g(x)$ 都收敛，则称此迭代公式 x^* 邻近具有局部收敛性。

定理 2 设 $g(x)$在 x^* 的邻域内有连续的一阶导数，且

$$|g'(x^*)| < 1$$

则迭代过程 $x_{k+1} = g(x_k)$ 具有局部收敛性。

在实际应用中，由于 x^* 事先不知，故条件 $|g'(x^*)| < 1$ 无法验

证，但根据 $g'(x)$ 的连续性，若已知根 x^* 就在初始值 x_0 的邻近，则可用条件 $|g'(x_0)|<1$ 来近代替代 $|g'(x^*)|<1$。下面看一实例：

例 8 求方程 $x=e^{-x}$ 在 $x_0=0.5$ 附近的解，要求精度 $\varepsilon=10^{-3}$。

解 由于 $|(e^{-x})'_{x=0.5}|\approx 0.6<1$，根据定理 2，$x_{k+1}=e^{-x_k}$ 收敛。为了满足精度 $|x^*-x_k|<\varepsilon$，根据定理 1，只需要求

$$\frac{L}{1-L}|x_k-x_{k-1}|<\varepsilon$$

即

$$\frac{3}{2}|x_k-x_{k-1}|<10^{-3}$$

故

$$|x_k-x_{k-1}|<0.000\,67$$

取初始值 $x_0=0.5$，计算结果列表如下：

k	x_k	x_k-x_{k-1}	k	x_k	x_k-x_{k-1}
0	0.5		6	0.564 86	−0.006 31
1	0.606 53	0.106 53	7	0.568 44	0.003 58
2	0.545 24	−0.061 29	8	0.566 41	−0.002 03
3	0.579 70	0.034 46	9	0.567 56	0.001 15
4	0.560 06	−0.019 64	10	0.566 91	−0.000 65
5	0.571 17	0.011 11			

由表可见，第 10 次迭代结果符合精度要求。

在实际计算中，也常常用 $|x_k-x_{k-1}|<\varepsilon$ 来控制迭代次数。

第三节　收集和分析数据的艺术

英国是现代统计学的发源地。英国《不列颠百科全书》上把统计学定义为收集和分析数据的艺术。人们在研究一个问题时，往往首先要收集资料。而资料往往是用数量形式表示的。这种形式的资料称为数据。怎样以有效的方式收集数据是统计学研究的中心问题之一。数据往往是杂乱无章的，很难看出其内在的规律性。整理、分析数据并由此对所研究的问题作出统计推断，为决策提供依据或建议是统计学研究的另一个中心问题。统计学研究数据，它是数学的一个分支。统计学研究的数据带有随机性，所以他的理论和方法有独到之处。学习统计重要的是领会统计思想，这样就能感受到统计的魅力。

1. 统 计 推 断

例 1　《今日美国报》和美国有线电视新闻网(CNN)1994 年 4 月 27 日公布一项民意测验调查结果：克林顿政府外交政策支持率为 39%；克林顿政府经济政策支持率为 45%。民意调查于 4 月 22 日至 24 日在 1 067 人中进行，其误差在 3%之内。(摘自 1994 年 4 月 28 日新民晚报)

在一个统计问题中，研究对象的全体称为总体，其中每个成员称为个体。在研究克林顿政府外交、经济政策支持率时，总体就是全体美国人，个体就是每一个美国人。对每一个美国人都作调查，这太花时间、人力和物力了。现从总体中抽取 1 067 人进行调查。这一抽取过程称为抽样。所抽取的部分个体称为样本。样本中个体的个数

称为样本容量。抽样的目的是通过样本了解总体，对总体的一些未知因素作出推断。在上例中，由于样本只有 1 067 人，仅用 2 到 3 天时间就调查完毕。根据样本中支持克林顿政府外交和经济政策的人所占的比例分别为 39%和 45%，推断出在全体美国人中克林顿政府外交和经济政策的支持率以及误差。

“误差在 3%之内”的完整含意是，“误差在 3%之内的可信度为 95%”。随机调查 1 067 人(样本容量)就是根据这个精度要求而计算出来的。如何收集数据，使得样本能够代表总体，这是最关键的问题。

例 2 (摘自 2000 年 10 月 13 日和 19 日文汇报)美国总统选举前的 10 月 11 日晚举行的第二场电视辩论后，CNN 迅速进行了民意测验。当晚就发布消息，称小布什赢得了本场辩论，49%的人认为小布什赢得了辩论，36%的人认为戈尔赢得了辩论。10 月 18 日举行的第三场电视辩论后，CNN 称戈尔稍占上风。46%的人认为戈尔赢得了这一场辩论，44%的人认为小布什赢得了辩论。考虑到民意测验的结果有 3%的误差，所以戈尔和小布什在第三场辩论中的表现没有显著的差异，很难说戈尔赢得了辩论。但是戈尔和小布什在第二场辩论中的表现确有显著的差异，确实是小布什赢得了这一场辩论。在统计推断中，只有当存在显著的差异时，才说两者有大小之别。否则只能说两者相等。

参数估计(包括点估计和区间估计)问题和假设检验问题是统计推断中的两大问题。例 1 给出的 39%和 45%分别是对克林顿政府外交和经济政策支持率的估计。由误差算得的区间[36%，42%]和[42%，48%]分别是克林顿政府外交和经济政策支持率的可信度为 95%的区间估计。例 2 是假设检验。这里有两个假设，一个称为原假设，另一个称为备择假设。原假设是戈尔和小布什没有显著的差异，两者相等；备择假设是戈尔和小布什有显著的差异，两者不相等。统计推断中的相等、不相等往往指的是两者有还是没有显著的差异。根据第二场电视辩论后 CNN 的调查结果，拒绝原假设，认为戈尔和小布什有显著的差异。在他们两人没有

显著差异的假设下，作出这样一个判断犯错误的可能性不超过5%。而根据第三场辩论后CNN的调查结果，不能拒绝原假设，认为戈尔和小布什没有显著的差异，当然这个判断也有5%犯错误的可能性。

2. 抽样调查

为了使样本能准确地推断总体，我们必须掌握科学的抽样方法。

(1) 选取样本时，谨防选择偏性

例3 1936年民主党人罗斯福任美国总统第一任期满，共和党人兰登与他竞选总统。《文学摘要》杂志根据有约二百四十万人参加的民意测验，预测兰登会以57%对43%的优势获胜。自1916年以来的五届总统选举中，《文学摘要》杂志都正确地预测出获胜的一方，其影响力很大。那时盖洛普刚刚设立起他的调查机构，他根据一个约五万人的样本，预测罗斯福会以56%对44%的优势获胜。实际结果是，罗斯福以62%对38%的优势胜出。当时有人说，这次选举的最大赢家不是罗斯福，而是盖洛普。自这之后，盖洛普的调查机构得到迅速的发展，国内外闻名，而《文学摘要》杂志不久就垮了。

罗斯福的得票率为62%，《文学摘要》杂志的预测为43%，误差达到19%。误差之大令人惊异。这样大的误差是怎么得来的呢？经过研究发现，原因在于《文学摘要》杂志选取样本有偏性。杂志是根据电话簿和俱乐部会员的名册，将问卷邮寄给一千万人。当时美国四个家庭中仅有一家装电话。他选取的样本有排斥穷人的选择偏性。这样的民意测验非常不利于民主党人罗斯福。

(2) 谨防不回答偏性

《文学摘要》杂志调查的一千万人中只有二百四十万人回答了问卷，不回答者可能非常有别于回答者，这二百四十万人代表不了被邮寄问卷的一千万人。1936年《文学摘要》杂志的一次专门的调查，给在芝加哥的选民每三人寄去一张问卷，约20%的被调查者作了回

答，其中支持兰登的超过半数。但是在选举中，兰登在芝加哥的得票率只有三分之一。所以当出现高不回答率时，谨防不回答偏性。当时的一次特别调查表明，低收入和高收入的人倾向于不回答问卷，因此中等收入的人在回答者中的代表性超出比例。为此现代调查机构更喜欢采用亲自询问来代替邮寄问卷，即使亲自询问，也有不回答偏性的问题。访问员来访时，不在家的人与在家接受访问的人可能在工作时间、家庭关系和社会背景等方面有比较大的差异，从而看法也不一样。例如有一项关于快餐的市场调查。抽取500户家庭进行调查。白天访问时，有150户家庭没人。能不能仅用白天有人的350户家庭的数据？不能。这里有不回答偏性。白天不在家的150户可能是吃快餐比较多的家庭。

1936年和之后的两次总统选举中盖洛普都正确地预测出获胜的一方。但是1948年的选举，他却预测错了。

(3) 人为选择样本时易带偏性

例 4 罗斯福逝世后，杜鲁门接任。1948年他任总统满期后，共和党人杜威与他竞争。盖洛普基于50 000人次的调查，预测杜威获胜，领先6个百分点。美国其余两家主要的民意调查机构也预测杜威获胜，领先5个百分点。实际结果是，杜鲁门以50%对45%的优势获胜。民意测验出了什么问题?

这三家民意测验机构全都采用定额抽样法。访问人员访问的人数是固定的，但访问的对象可由访问人员自由选定。例如盖洛普要求在 St. Louis 城访问的人员要访问13个对象，规定其中：

6人住在近郊，7人住在市中心；

男性7人，女性6人；

在7个男性中，3人40岁以下，4人40岁以上；1个黑人，6个白人。

对女性也有类似的定额规定。

结果，1948年的民意调查访问人员选择了过多的共和党人。这是因为共和党人较为富裕，受过较好的教育，住在较好的街区，他们较易访问，所以访问人员喜欢采访共和党人。这造成了民意测验中

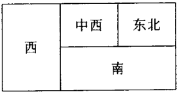
有利于共和党的偏性。下面的表体现了这种偏性：

年份	共和党实际得票率(%)	盖洛普预测共和党得票率(%)	有利于共和党的误差(%)
1936	38	44	6
1940	45	48	3
1944	46	48	2
1948	45	50	5

(4) 用概率方法去选择样本

1952 年之后，盖洛普采用概率方法去选择样本，即分层多阶抽样的方案。他有以下六个步骤。

第 1 步，将美国分为四层，即四个地理区域：东北、南、中西、西。



第 2 步，将每一个地理区域分成一个个城镇。例如在东北地区，将人口在 5 万到 25 万的居民中心区归成城镇。在每一个地理区域内随机抽取若干个城镇。

第 3 步，将城镇划分成选区。在每一个选出的城镇内随机抽取若干个选区。

第 4 步，将选区划分成选分区。在每一个选出的选区内随机抽取若干个选分区。

第 5 步，在每一个选出的选分区内随机抽取若干个家庭。

第 6 步，最后访问选出的家庭中的某些成员。此时，访问员会接到通知，例如要求他与家庭中 18 岁以上的最年青的男子交谈，若没有男子在家，则与 18 岁以上的最年长的女子交谈等。

(5) 定额抽样法和用概率方法去选择样本的比较

用概率方法去选择样本消除了定额抽样法的缺点，防止了访问

员的选择偏性。

定额抽样法的原意是为了保证对样本的一些要求，使得样本中的比例适当，但由于访问员的判断和选择往往带有偏性，这个要求不一定能满足。而概率方法是不带偏性的，它要求接近总体的情况。例如样本中黑人的比例，年青人的比例，生活水平低下的人的比例等与总体中的比例相近。

1948年之前，盖洛普民意测验使用定额抽样法，调查50 000人。1948年后用概率方法去选择样本，调查样本的容量只有原先的五分之一到十分之一。按美国人口平均，用概率方法在十万人中调查的样本不到5人。不但样本容量下降了很多，而且由于没有偏袒任何一方（共和党或民主党）的倾向，精度也提高了很多。1936到1948年的误差大约为5%，1948年之后要小得多。看下面的表。

1948年后盖洛普民意测验在总统选举中的预测情况

年份	样本容量	获胜总统	盖洛普预测得票率	选举结果	误差
1952	5 385	艾森豪威尔	51%	55.4%	+4.4%
1956	8 144	艾森豪威尔	59.5%	57.8%	−1.7%
1960	8 015	肯尼迪	51%	50.1%	−0.9%
1964	6 625	约翰逊	64%	61.3%	−2.7%
1968	4 414	尼克松	43%	43.5%	0.5%
1972	3 689	尼克松	62%	61.8%	−0.2%
1976	3 439	卡特	49.5%	51.1%	+1.6%
1980	3 500	里根	55.3%	51.6%	−3.7%
1984	3 456	里根	59.0%	59.2%	0.2%
1988	4 089	布什	56.0%	53.9%	−2.1%

(6) 全面调查和抽样调查

和全面调查相比较，抽样调查具有如下特点：

1) 抽样调查的费用较低、速度较快、应用面较广。

2）由于可以较严格地挑选和培训调查员，调查和数据处理的质量比较容易控制，而且被调查者的心理压力较小，因此抽样调查可获得较准确的结果。

3）当调查对象非常多甚至无限，或测试方法具有破坏性时，根本无法进行全面调查，只能进行抽样调查了。

3. 对 照 实 验

除了抽样调查之外，实验是收集数据的另一个重要方法。众所周知，抛掷一枚均匀的硬币，出现正面和反面的可能性都为 0.5。那么抛掷一枚图钉，钉尖朝上和朝下的可能性各为多大？他们是否相等？解决这个问题的最为简单的办法是做实验。将一把图钉抛掷很多次，计算钉尖朝上出现的频率。从而得到钉尖朝上的可能性。通过实验人们认为这个值为 $\frac{13}{20} = 0.65$。从而得到钉尖朝下出现的可能性为 0.35。

对照比较是测试一种新药效果的最基本的办法。以随机的方式将病人分到处理组或对照组。把药分给处理组的病人，而对照组的病人不接受治疗，然后比较两个组的反应。整个实验在双盲的情况下进行，这也就是说，不管是病人，还是医生都不知道谁在处理组，谁在对照组。

脊髓灰质炎俗称小儿麻痹症。20 世纪 60 年代前，脊髓灰质炎是令人惧怕的疾病之一，严重危害着儿童的健康。1954 年美国公共卫生总署决定组织脊髓灰质炎疫苗实验。实验对象是一、二、三年级的儿童。提出的第一个实验方案是，给大量儿童接种疫苗，如果 1954 年脊髓灰质炎发病率比 1953 年明显下降，就是说疫苗有效。但是经过论证认为这个实验方案不可行。脊髓灰质炎是一种年发病率变化很大的流行病。1952 年有 60 000 个病例，而 1953 年只有其一半。1954 年的低发病率可能说明疫苗有效，也可能说明当年发病率本来就低。

第二个方案是，取得父母同意的儿童接种疫苗，组成处理组，其他儿童组成对照组。这个方案可能引起疫苗的偏性，因为高收入家庭的父母比低收入家庭的父母更赞成接种疫苗，而高收入家庭的儿童更易受到脊髓灰质炎的伤害。

第三个方案是小儿麻痹症全国基金会提出的。该方案给所有二年级的并取得父母同意的儿童接种疫苗，而将一、三年级的儿童留作对照。这个方案有以下两个不足之处：

第一是脊髓灰质炎是通过接触传染，所以二年级的发病率有可能比一或三年级的发病率高，这将使研究结果不利于方案。也有可能二年级的发病率比一或三年级的发病率低，这将使研究结果有利于方案。

第二是将取得父母同意的儿童放在处理组，这将造成一个不利于方案的偏倚。

最后一个方案是随机化对照比较双盲实验。该实验的处理组和对照组都来自父母同意接种疫苗的儿童们。将这些孩子分配到处理组或对照组的方法有以下两个：

第一种方法是人事判断，以使得处理组和对照组中的家庭收入，儿童的健康状况、性格以及兴趣的情况相近。当对象很多时，人事判断费时、费力且经济上不合算，常会出现偏差。

第二种方法，也是较恰当的方法是随机分配。扔一枚均匀的硬币，以 50%对 50%的机会将儿童分配到处理组或对照组。随机法则保证了处理组和对照组中所有重要的变量的情况非常相近。

实验为什么要双盲？为什么不让儿童（包括他的父母）以及医生知道谁在处理组谁在对照组呢？这是因为如果实验对象不知道他们是在处理组还是在对照组，他们的反应是对疫苗的，而不可能是对处理或对照的意见。由于医生在实验期间必须检查孩子是否感染了脊髓灰质炎，而脊髓灰质炎的症状是难以诊断的，在不易确定时，医生的诊断可能会受到事先知道孩子是否接种过疫苗的影响。

随机化对照比较双盲实验和小儿麻痹症全国基金会方案都得到

了实施，实验结果如下表所示：

随机化对照比较双盲实验

	人　数	病　例　数	每十万人中的病例数
处理	200 745	57	28
对照	201 229	142	71

小儿麻痹症全国基金会方案

	人　数	病例数	每十万人中的病例数
2 年级(接种疫苗)	221 998	56	25
1、3 年级(对照)	725 173	391	54
2 年级(不同意)	123 605	54	44

小儿麻痹症全国基金会方案中的处理组仅仅包含那些父母亲同意接种疫苗的儿童，而对照组还包含那些父母亲不同意接种疫苗的儿童。处理组和对照组的差异可能来自于疫苗，也可能来自于其它因素。疫苗的效应和其他因素的效应混淆在一起。混淆是产生偏性的主要根源。在小儿麻痹症全国基金会方案的实验结果中，疫苗使脊髓灰质炎的发病比例从十万分之五十四降到十万分之二十五，如果将二年级中父母不同意的儿童组成对照组，则疫苗使脊髓灰质炎的发病比例仅从十万分之四十四降到十万分之二十五。而随机化对照比较双盲实验的实验结果中，疫苗使脊髓灰质炎的发病比例从十万分之七十一降到十万分之二十八。小儿麻痹症全国基金会方案对疫苗的研究有偏向于不利于疫苗的方面。随机化对照比较双盲实验比小儿麻痹症全国基金会的方案好。

如果假设疫苗没有效果，那么处理组和对照组中脊髓灰质炎的发病比例应大致相等。在疫苗没有效果时，造成十万分之七十一和十万分之二十八这样一个大的差异的可能性是十亿分之一。这说明疫苗是有效的。这是个假设检验问题，原假设是疫苗没有效果，备择假设是疫苗有效果。由于在疫苗没有效果时，十万分之七十一和十万分之二十八的差异非常显著，造成这样一个大的差异的可能性仅是十亿分之一。我们拒绝原假设，认为疫苗有效。

4. 统 计 分 析

统计分析的目的是探索数据内在的数量规律性。英国的约翰·格朗杰(Joun Grannt)在 1662 年出版了《关于死亡表的自然观察与政治观察》一书，对现代统计学的发展作出了重要的贡献。他通过大量调查、观察和研究，发现了人口与自然现象中的一些数量规律。如新生儿的男女性比例为 14∶13；男性在各年龄组中死亡率普遍高于女性；新生儿和大城市人口的死亡率较高；一般疾病和事故的死亡率较稳定，而传染病的死亡率波动较大等等。他根据伦敦市的人口调查资料，发表了世界上最早的一张生命表。

生 命 表

年 龄(岁)	生 存 数	死 亡 数
0—5	100	36
6—15	64	24
16—25	40	15
26—35	25	9
36—45	16	6
46—55	10	4
56—65	6	3
66—75	3	2
76—85	1	1

虽然这张生命表很粗糙，但是他的编制格式沿用至今。

例 5 下表是 1976 至 1977 年美国佛罗里达州 29 个地区杀人案件中被告肤色和是否被判死刑的 326 个犯人的调查情况。

被 告	死 刑		死刑判决的比例
	是	否	
白 人	19	141	0.119
黑 人	17	149	0.102

从表中看，白人被判死刑的比例较高，这与当时美国的现实情况不相符。后来人们除了考虑被告人的肤色外，还考虑被害人的肤色，得到的结论就与当时美国的现实情况相符了。如下的表是上面这张表的细分。

被害人	被　告	死　刑		死刑判决的比例
		是	否	
白　人	白人	19	132	0.126
	黑人	11	52	0.175
黑　人	白人	0	9	0.000
	黑人	6	97	0.058

如果被害人是白人，白人被判死刑的比例为 12.6%，而黑人被判死刑的比例为 17.5%。如果被害人是黑人，白人被判死刑的比例为 0，而黑人被判死刑的比例为 5.8%。这说明，无论被害人是白人还是黑人，白人被告被判死刑的比例都比黑人被告被判死刑的比例低。尤其是在被害人是黑人时，白人被告没有被判死刑的。这说明在美国有种族歧视，死刑判决与被害人的肤色有关。

这个例题的前一张表仅考虑被告的肤色和是否被判死刑的关系，被害人的肤色就是隐蔽着的混杂因素，它误导了统计分析。这个问题就是统计中著名的 Simpson 悖论的一个实例。

结论 1　白人被判死刑的比例大于黑人被判死刑的比例。

结论 2　在被害人是白人时，白人被判死刑的比例小于黑人被判死刑的比例；在被害人是黑人时，白人被判死刑的比例小于黑人被判死刑的比例。

显然，结论 2 与事实相符，而结论 1 是误导出来的结论。为避免发生这种现象，找到隐蔽着的混杂因素至关重要。这除了依靠统计学的方法外，还要依靠有关的专门知识。找到了隐蔽着的混杂因素后，一般的处理方法是对混杂因素的每一个值（如被害人的肤色），都构造一张表（如被害人是白人时的表和被害人是黑人时的表）。然后对这些表进行分析比较。这种方法称为控制混杂因素。当然我们也

可以把被告的肤色视为被控制的因素，得到如下的表：

被　告	被害人	死　　刑		死刑判决的比例
		是	否	
白　人	白人	19	132	0.126
	黑人	0	9	0.000
黑　人	白人	11	52	0.175
	黑人	6	97	0.058

无论被告是白人还是黑人，被害人是白人时凶手被判死刑的比例都比被害人是黑人时明显的高。如果删除凶手的肤色这个属性，则得到如下的表：

被害人	死　　刑		死刑判决的比例
	是	否	
白　人	30	184	0.140
黑　人	6	106	0.053

被害人是白人时凶手被判死刑的比例比被害人是黑人时也明显的高。这时 Simpson 悖论不再成立。

下例是 Simpson 悖论的另一个实例。

例 6　根据 1990 年第四次人口普查资料，研究文化程度与死亡率的关系。不同文化程度的死亡率如下表所示：

	居民人数	死亡人数	死亡率(‰)
文　盲	1 461 971	43 085	29.470
小　学	1 870 095	21 917	11.720
初　中	3 113 930	10 741	3.449
高中、中专	2 091 845	4 038	1.930
大专、大学	687 195	1 991	2.897

总的来说，文化程度高了，死亡率降低，但是高中和中专文化程度的死亡率最低。情况是否果真如此？观察对象(人)除了已经考虑

的因素(文化程度和死亡率)之外,在其他方面(如年龄)也有所不同。比较不同年龄组内高中、中专和大专、大学文化程度的死亡率,看看青年人、中年人和老年人中高中和中专文化程度的死亡率是否也是比大专和大学低?得表如下:

年龄	高中、中专			大专、大学		
	居民人数	死亡人数	死亡率(‰)	居民人数	死亡人数	死亡率(‰)
25—29	573 426	227	0.396	126 892	40	0.315
30—34	766 924	381	0.497	88 318	24	0.272
35—39	163 206	111	0.680	89 555	34	0.380
40—44	175 494	197	1.123	97 436	64	0.657
45—49	138 857	239	1.721	85 847	123	1.433
50—54	87 539	281	3.210	75 622	179	2.367
55—59	75 524	372	4.926	52 853	205	3.879
60—64	48 688	391	8.031	31 199	203	6.507
65—69	31 860	457	14.344	19 345	236	12.200
70—	30 327	1 382	45.570	20 218	883	43.674

在各年龄组内大专、大学文化程度的死亡率都比高中、中专的死亡率低。再看下表。它表示不同年龄组内文化程度和死亡率(‰)的关系。

不同年龄组和文化程度的死亡率(‰)

年龄	文盲	小学	初中	高中、中专	大专、大学
25—29	5.499	1.112	0.724	0.396	0.315
30—34	3.354	1.319	0.897	0.497	0.272
35—39	2.055	1.392	1.038	0.680	0.380
40—44	2.940	1.893	1.511	1.123	0.657
45—49	3.198	2.924	2.490	1.721	1.433
50—54	4.537	4.518	3.952	3.210	2.367
55—59	6.835	7.310	6.289	4.926	3.879
60—64	11.686	12.467	10.505	8.031	6.507
65—69	19.710	21.228	17.975	14.344	12.200
70—	76.194	63.100	55.027	45.570	43.674

从表中可见，在各年龄组内都显示出文化程度越高，死亡率越低的规律。如果仅考虑文化程度和死亡率这两个属性，就得出了高中和中专文化程度的死亡率最低的结论。如果将年龄因素也考虑进去后，就得到了大专、大学文化程度的死亡率最低的结论。显然后一个结论是合理的，因为年龄是影响死亡率的关键因素，必须加以考虑。

为什么死亡率随着文化程度的提高而降低？通过数据分析发现了规律性。但是统计学并不能解释发现的规律性，还要依靠有关专门学科进一步的研究。例如，数据分析显示，吸烟的人中患肺癌的比例较高。为什么吸烟会诱发肺癌？这需要医学作出解释。使用统计方法解决实际问题时，首先要了解问题的背景和研究目的。对于统计分析的结果要做出符合实际的解释，以便进一步深入的研究。

习题

1. 为了解学生晚上看电视的情况，在参加早上锻炼的学生中进行调查。根据这样调查得到的数据进行分析，所得结论可信吗？

2. 1988 年 9 月 11 日，美国 The San Francisco Examiner 报刊登了一则消息，标题是：10 名生物教师中有 3 人相信上帝创世说。他们从全国教师协会提供的名单中随机抽取 20 000 名高中生物教师，然后将问卷寄给他们。共收到 200 份答卷，其中百分之三十的生物教师相信上帝创世说。这个结论可信吗？

3. 美国加利福尼亚大学伯克莱分校研究生的入学录取情况如下：

专业	男		女	
	申请人数	录取率(%)	申请人数	录取率(%)
A	825	62	108	82
B	560	63	25	68
C	325	37	593	34
D	417	33	375	35
E	191	28	393	24
F	373	6	341	7
合计	2 691	44	1 835	35

试对该校录取新生中的性别歧视问题进行讨论。

4. 乳腺癌是妇女常见的恶性肿瘤之一。在癌扩散之前及早发现，治疗成功的机会是否更好？为此，全纽约健康保险规划于 1963 年实施了一次大规模的实验。实验对象为规划中的所有成员，共 62 000名 40 到 64 岁的妇女，她们被随机地分成两个人数一样的组。处理组中有 20 200 名妇女接受了由医生和 X 光进行的检查，有 10 800名妇女拒绝检查。对照组中的妇女都接受了普通健康检查。所有妇女被跟踪了若干年，头五年的死亡人数、死亡原因和死亡率如下表所示：

	死亡原因			
	乳腺癌		其它	
	人数	死亡率(‰)	人数	死亡率(‰)
处理组				
检查 20 200	23	1.1	428	21
拒绝 10 800	16	1.5	409	38
总数 31 000	39	1.3	837	27
对照组 31 000	63	2.0	879	28

(1) 检查对健康有利吗？表中哪几个数据证明了你的观点？

(2) 在处理组中，拒绝检查妇女中的总死亡人数为 425，而接受检查妇女中的总死亡人数为 451。拒绝检查妇女中的死亡率大约是接受检查妇女中的死亡率的将近 2 倍。检查使死亡率降低了一半吗？为什么？

(3) 该研究是双盲的吗？

(4) 在实验的第一年里，在接受检查妇女中发现了 67 例乳腺癌，拒绝检查妇女中发现了 12 例，而在对照组中发现了 58 例，能否说检查引起乳腺癌？

参考文献

陈希孺.统计学概貌.科学技术文献出版社,1989年.

David Freedman.统计学.魏宗舒译.中国统计出版社,1997 年.

Judith Tanur.统计学应用指南.陈湛匀译.上海人民出版社,1990 年.

袁卫.描述统计学.中国统计出版社,1996 年.

第四节　池塘里有多少鱼

——从超几何模型谈起

我们首先从概率论中一些容易理解而且有实际意义的问题出发，引出一种简单的概率模型——超几何分布。通过分析解决问题的过程，去理解概率统计中的一些基本概念和方法以及应用的想法；其次通过简化计算的需要，引出二项分布，进一步说明概率论在数学及其应用的发展中的一些作用；最后从有限个独立的两点分布(Bernoulli 分布)过渡到无限个独立的两点分布，引出随机游动、渗流和吉布斯随机场等这些当代概率论研究的热点问题。希望通过以上的介绍，使读者比较容易地了解或理解概率论与数理统计的一些基本概念和应用的想法，同时也可以看到在初等数学与高等数学甚至是近代的研究课题之间存在着程度不同的联系。对于中学教师来说，则希望能为他们提供一个例子，并通过他们的教学，使中学生不但能够学会数学的基本知识和技能，更能提高思维方面的修养，引起他们对近代数学及其应用的兴趣和遐想。

1. 超几何模型及其应用

(1) 问题及最初步的解答

例 1　从一个池塘里捞出 1 000 尾鱼，将其尾部标以红点，仍然放入水中。经过一段时间，再从池中捞出 1 000 尾鱼，其中有红点的鱼有 100 尾。试估计池中有多少条鱼？

例 2　由厂方提出的一箱产品计 1 000 件，从中取出 100 件，发现其中有 2 件不合格品。经约定：如果一箱的废品率超过 1%，那么买方

就不接受此(整)箱产品;否则买方就得接受。问此箱产品应否接收?

上述问题是有普遍意义的,其中的具体数字只是为了说明时的方便。对于例 1,实际上可以广泛地用在估计未知总体数(如野生生物资源的调查)的问题上。例 2 是产品检验的一个典型例子,它不但对产品的检验有用,而且也可以在生产过程中用于控制产品质量。所以是有重要的应用意义的。

我们先从生活常识的角度对例 1 进行分析而得到最初步的答案如下:

将标有红点的 1 000 尾鱼再放入水中以后,鱼的总数未变。经过一段时间,这些鱼在池中应该分布"均匀"了,而第二次捞出的鱼中有红点者占捞出鱼总数的 $\frac{100}{1\,000} = 10\%$。所以从比例的观点看,池中鱼的总数 x 应该满足

$$x \times 10\% = 1\,000$$

所以 $x = 10\,000$,因而可以认为池中的鱼大约在万尾左右。

例 2 的解决也可以从比例的观点出发,认为此箱产品的废品率为 $\frac{2}{100} = 2\%$,它大于 1%,因而按照规定买方可以拒绝接收。

事实上例 2 的废品率很可能不超过 1%,如果买方拒绝接收,那么一般来说,厂家就会对整箱产品逐个检查,找出箱中所有的废品。这样自然就会大大增加检查的费用,更何况有时成品的质量检查是破坏性的,如灯泡的寿命指标的检验便是这样。因此提出了以下问题:能否有某种办法可以更合理地处理这类问题?对于例 1,也有一些更深入的问题值得研究。

(2) 上述两个例题的一般模型

1) 在上述两个例题中,所考察的个体(鱼,产品)的全体(总体)个数都是一个有限数 N。我们将所考察的个体通称为"球",并且认为都在一个"袋"之中。例 1 和例 2 中的 N 分别为未知和 1 000。

2) 在两个问题中,总体的元(个体)都分成两类(有红点或无红点;废品或合格品),将前者通称为"红球",后者通称为"黑球"。记红

球的个数为 M,则例 1 和例 2 中的 M 分别为未知和 1 000。

3) 在两个问题中,都从总体中抽出若干个球(一个样本),样本的容量(所含元的个数)n 在例 1 和例 2 中分别为 1 000 和 100。

4) 在两个问题中,样本中含有红球的个数 m 在例 1 和例 2 中分别为 100 和 2。

5) 假设从总体中抽取任意一球的可能性都相等。

归纳上述分析,我们得到以下的超几何模型:

设有一袋,袋中有 N 个球,其中有 M 个红球,$N-M$ 个黑球,假设从袋中抽取任意一球的可能性相等。现从袋中任取 n 个球,用 X 表示取出的 n 个球中的红球数,问随机事件 $\{X=m\}$ 的概率是多少? 其中 $m=1,\ 2\ \cdots\ n$。

上述模型的基本事件数为

$$\binom{N}{n}=\frac{N(N-1)\cdots(N-n+1)}{n!}$$

其中 n 为非负整数,N 可以是任何实数;当 $n\leqslant N$ 且 N 为正整数时,$\binom{N}{n}=C_N^n$;当 $n>N$ 且 N 为正整数时,$\binom{N}{n}=0$。所以它是组合数记号的一个自然推广,而且比组合数记号更好用。事件 $\{X=m\}$ 与事件“n 个球中恰有 m 个红球”和事件“有 m 个红球,$n-m$ 个黑球”是相同的。而 m 个红球只能从 M 个红球中取,$n-m$ 个黑球只能从 $N-M$ 个黑球中取,由于 m 个红球的任意一种取法都可以和 $n-m$ 个黑球的任一种取法相配成为 n 个球中恰有 m 个红球的一种取法,所以 $\{X=m\}$ 包含的基本事件数为 $\binom{M}{m}\times\binom{N-M}{n-m}$。故由古典概率的定义有

$$P(X=m)=\frac{\binom{M}{m}\times\binom{N-M}{n-m}}{\binom{N}{n}}\qquad m=0,\ 1,\ \cdots,\ n \qquad ①$$

(3) 随机变量 X 的分布

首先 X 是一个变量,可能取值是 $0, 1, \cdots, n$ 中的一个。如果用 Ω 表示超几何分布模型的基本事件空间,那么对它的任何基本事件 $\omega \in \Omega$ 来说,其中的红球个数是完全确定的,这个确定的数就是 X 的值。因此根据函数的定义,X 是基本事件空间 Ω 上的函数。这种定义在基本事件空间 Ω 上的函数称为随机变量(注:如果基本事件空间无限,还应验证该函数的可测性,在此不再讨论)。但是从问题的实际意义来考察,它又与以往我们遇到的函数不同。那就是当随机试验(即抽球)尚未实施时,X 究竟取哪一个值是随机的(即带有偶然性)。那么这种取值带有偶然性的函数——随机变量用什么数学工具来刻划和研究呢?我们就用它取值的概率(可能性)来研究。即用概率 $P(X=m)$ 作为研究随机事件 $\{X=m\}$ 的数学工具。称①为随机变量 X 的概率分布,它全面反映了 X 取值的概率规律。我们将这个特殊的概率分布①称为超几何分布。

从学科上讲,研究随机现象的数学称为概率论。随机事件和事件的概率是概率论的基本概念,而随机变量及其概率分布则是建立在它们基础上的最重要的基本概念之一。在概率论中,还引进随机变量或分布的各种数字特征来刻划它们某些特性;研究随机变量的函数的性质;随机变量序列的极限性质等都是研究静态随机现象的基本内容。为了研究动态随机现象,还引进了随机过程,即以时间为自变量而值为随机变量的随机函数,进而在随机过程的基础上研究各种理论问题,提出了各种研究方法。同时还将概率论和随机过程的理论与方法应用于科学技术、经济和管理等各个方面。形成了分支众多蓬勃发展的现代概率论。

(4) 总数 N 的最大似然估计

我们先对例 1 进行讨论。

在例 1 中,M、n、m 是已知的,N 是未知的。所以①式中的 $P(X=m)$ 是 N 的函数。一个直观的想法是:N 应该使概率 $P(X=m)$ 达到最大。为便于讨论,将它记作 $q(N; M, n, m)$,考虑当 N 上升时,它的升降情况。通过计算比值得到

$$\frac{q(N-1;\ M,\ n,\ m)}{q(N;\ M,\ n,\ m)}=1+\frac{mN-nM}{(N-n)(N-M)}。$$

因而

$$q(N-1;\ M,\ n,\ m)\begin{cases}<q(N;\ M,\ n,\ m) & Nm<Mn\\ =q(N;\ M,\ n,\ m) & Nm=Mn\\ >q(N;\ M,\ n,\ m) & Nm>Mn\end{cases}$$

因此,当 $N=\frac{Mn}{m}$ 为整数时,q 在 $N=\frac{Mn}{m},\ \frac{Mn}{m}-1$ 处达到最大;当 $N=\frac{Mn}{m}$ 不是整数时,q 在 $N=\left[\frac{Mn}{m}\right]$ 处达到最大。根据以上想法,我们得到例 1 的结论:池塘里应该有鱼

$$N=\frac{1\ 000\times 1\ 000}{100}=10\ 000\ \text{尾}$$

虽然这个结论与以前按比例观点求出的相同,但是它是基于一种更令人信服的分析。更重要的是:这种想法是一种具有广泛应用的方法和想法——最大似然思想的一个应用。

(5) 废品率的假设检验

首先将超几何模型中的球看成产品,红球和黑球分别看成合格品和废品。产品检验的问题是这样提出的:产品总免不了有废品,在买卖中,买方当然希望买进的货物中废品尽量地少,而卖方则希望合格品都被买方接受。最自然的办法是由买卖双方对产品逐个检验。这种办法只能适用于非破坏性的检验(即产品被检验后不影响质量),而且批量小、检验费用低的情况。在现代化生产和市场交易中,这种情况是很少的。货物经常是成批交付的。因此人们希望制定一种比较简便的验收方案,使买卖双方在每批货物的交接中,尽可能都得到满足。即对于卖方交付的每批产品,通过检验其中部分产品,使买方接收的废品比例和卖方被退回的合格品的比例都在可以接受的限度之内。这类通过检验部分产品的验收方案统称为抽样检验方案。

为了理解建立这种方案的想法，我们还是从例 2 开始。假设例 2 中所检验的那箱产品的废品率是 1%，那么由①式知，此时

$$N = 1\,000,\ n = 100,\ M = 1\,000 \times 1\% = 10$$

$$P(X \leqslant 3) = \sum_{m=0}^{3} P(X = m)$$

$$= \sum_{m=0}^{3} \frac{\binom{10}{m} \times \binom{990}{100-m}}{\binom{1\,000}{100}} = 0.987\,67 \qquad ②$$

这就是说，$P(X > 3) = 1 - 0.987\,67 = 0.012\,33$，即抽到 3 个以上的废品的概率(可能性)是很小的(1.23%)；而且还可以证明，当废品率小于 1%时，抽到 3 个以上的废品的可能性更小。根据实践经验知道概率很小的事件是难于发生的，所以从卖方希望尽量将合格箱交出去的观点看：从一箱产品中抽取 100 个产品，抽到的废品数大于 3 时，就没有理由交给买方，卖方应该自己留下；抽到的废品数小于或等于 3 时，就可以认为此箱产品合格，买方应该接收(因此例 2 的那一箱产品应该认为是合格品)。于是按照卖方的观点应该约定：从一箱产品中抽取 100 个产品，抽到废品数大于 3 时，卖方应该自己留下；抽到的废品数小于或等于 3 时，就应该认为该箱产品合格，买方应该接收。由于“概率很小的事件在实践中难于发生”，所以在统计学研究问题时就认为它不发生而往下进行推断。这种推断的办法在统计学中称为实际推断。有的书直接提出以下的实际推断原理：

一个事件如果发生的概率很小(例如 1%或 5%)，那么在一次试验中，就认为它不会发生；反之，一个事件如果发生的概率很大(例如 99%或 95%)，那么在一次试验中，认为它必定发生。

(6) 抽样推断的两类错误

事实上，事件发生的可能性小、难于发生，并不等于不发生。所以存在这样的情况：抽到的废品数虽然大于 3，但该箱的废品率不超过 1%。此时，虽然此箱产品合格，但是按照约定，还得作为不合格

处理而招致损失。于是卖方损失的可能性达到 1.233%（即 $P(X>3)$）。这个 1.233%是一箱产品的废品率小于规定的 1%而被错误地判断为不合格的概率，在统计学中称为犯第一类错误的概率，或者称为弃真概率。

以上只是从卖方的角度来考虑问题，我们现在从买方的角度加以分析：卖方交出产品只是根据假设所检验的箱合格做出的断言，该箱产品完全可能不合格。买方当然十分关心接收不合格的箱的概率有多大？这个概率通常称为犯第二类错误的概率或纳伪概率，买方总是希望纳伪概率尽可能小。按照超几何分布，此例的纳伪概率应该是：在废品率超过 1%，即 $M>1\,000\times1\%=10$ 的条件下，概率

$$P(X\leqslant3)=P_M(X\leqslant3)=\sum_{m=0}^{3}\frac{\binom{M}{m}\times\binom{1\,000-M}{100-m}}{\binom{1\,000}{100}}$$

经计算得知：

M	11	13	20	30	40	50
$P_M(X\leqslant3)$	0.982 1	0.817 75	0.588 54	0.229 76	0.038 16	0.010 78

由上述计算结果可以看出：在样本容量 100，废品率超过规定 1%而小于或等于 3%时，纳伪概率都很大。这种情况使得卖方认为买方应该接受的产品，而买方却不能接受。但是从买方的观点看，他也可以规定一个能接受的“最坏”（即使得产品的质量达到他可以接受的最低程度）的废品率，而使纳伪概率较小。人们称这个“最坏”的废品率为极限质量，通常记作 p_1。而将原来双方约定的废品率称为合格质量，记作 p_0。从上面的计算结果可知：如果极限质量规定为 4%，那么纳伪概率不超过 3.8%。如果极限质量规定为 5%，那么纳伪概率不超过 1%。

（7）抽样检验方案

以上的讨论可以总结如下：设想交的每批产品数（也称产品的批量）为 N，产品的抽样检验方案就是：规定每批产品抽验的产品数 n

和其中允许废品数的上限(也称合格品判定数)c。如果抽出的 n 件产品中的废品数 X 小于或等于 c,这批产品就由买方整个接收;如果 X 大于 c,买方就拒收这批产品。

为以后叙述简单起见,将这个方案记作(n, c)。称为计数标准型一次(n, c)抽样检验方案,简称(n,c)抽样检验方案。方案(n, c)的确定方法如下:

从卖方的观点看,“理想”的方案是:确定一个数 $p_0 \in (0, 1)$ (称为合格质量),如果一批产品中的废品数 $M \leqslant Np_0$ 时,就认为这批产品合格。对卖方来说,方案的要求是:给出较小的正数 α(即弃真概率,通常取 0.01 或 0.05),使得 n、c 满足

$$P(X \leqslant c) \geqslant 1-\alpha,\ M \leqslant Np_0 \qquad ③$$

从买方的观点看,确定一个数 $p_1(\geqslant p_0)$ (称为极限质量),如果一批产品中的废品数 $M \geqslant Np_1$ 时,就认为这批产品不合格而加以拒绝。和上面的道理类似,对买方来说,方案另一要求是:对给出较小的正数 β(即纳伪概率,通常取 0, 01 或 0, 05),使得 n、c 满足

$$P(X \leqslant c) \leqslant \beta,\ M \geqslant Np_1 \qquad ④$$

又可以证明: $P(X \leqslant c)$ 随废品数 M 的上升而下降。再由实际情况,不妨设 Np_0, Np_1 都是整数。所以满足①, ②的 n、c 就是满足

$$P(X \leqslant c)\begin{cases} \geqslant 1-\alpha & M = Np_0 \\ \leqslant \beta & M = Np_1 \end{cases} \qquad ⑤$$

如果③中的概率使用超几何分布算出,那么由超几何分布的公式知 n、c 是下列不等式组的最小整数解:

$$\sum_{m=0}^{c} \frac{\binom{Np_0}{m} \times \binom{N(1-p_0)}{n-m}}{\binom{N}{n}} \geqslant 1-\alpha$$

$$\sum_{m=0}^{c} \frac{\binom{Np_1}{m} \times \binom{N(1-p_1)}{n-m}}{\binom{N}{n}} \leqslant \beta \qquad ⑥$$

这一组不等式并不能直接解出，通常只能通过试算求解。现在的办法是：当 N 较小时，将超几何分布的数值都计算出来，并制成表，需要时通过查表来求出 n、c。当 N 较大时，将超几何分布用接近于它的并且较易于计算的分布来代替，然后来解不等式组(4)。这一点成为许多基本分布产生的背景。顺便说一句，讨论分布之间的接近程度和分布的极限也是概率论的主题之一。

(8) 问题中的统计思想

从提出超几何分布的两个应用一直到制订(n, c)抽样验收方案行文虽然是显得长了一些，但是这里包含了很多重要的统计思想和观念。我们在这里作一些归纳，对于没有学习过统计的读者可以对它的一些重要方面有初步的了解，对于那些学习过统计的读者，也许可以通过这个简单的例子加深理解和了解。

超几何分布的第一个应用是：球的总数未知，红球数已知，要通过抽取(观察)部分球(样本)的情况来估计总数。第二个应用是：球的总数知道，抽取(观察)一部分球，希望通过清点这一部分球中的红球数，来探讨全体球中有多少红球。归纳起来，就是希望运用数学方法，通过样本的数据来判断总体的某些性质。其实，这就是统计学研究的对象。

由于统计学的基本问题和主要内容是由对象的部分现象来推断全体的现象，因此可以说它的推断是归纳性的，它对所研究的对象的结论不是决定性的，带有一定的随机(偶然)性，而且还有犯错误的可能。但是，这类问题的结论是用概率的概念表达的，这些结论是数学的，是决定性的，确立这些结论的方法是数学(不一定从一开始就是数学)的。所以一般认为统计学的基本思想与数学有很大的不同，但是它的方法论的基础是数学。因此有人认为统计学是数学的一个分支，也有人认为它应该从数学中独立出来。但是无论如何，在它的发

展过程中，既要把握统计思想，注意它的广泛应用，又要特别注意数学模型的建立和方法的运用。

前面的讨论实际上涉及统计学的两个部分：例 1 实际上是研究统计学的参数估计，而所用的方法就是最大似然方法；例 2 实际上是应用统计学中假设检验的思想。参数估计和假设检验是数理统计的基本理论部分，是统计学的基础。而最大似然法的思想则是近现代统计推断理论中最重要而且影响最大的方法之一。产品验收只是质量控制中的一个问题，质量控制或全面质量控制是现代化生产、贸易和管理的一个十分重要而有用的分支。

从统计学的角度来看，例 1 和例 2 的讨论也涉及了统计学的抽样和抽样分布问题。“抽球”就是统计中最简单的抽样方法之一，即不放回抽样。就是说，抽取 n 个球可以设想是每次抽一个，但抽出后不放回，而连抽 n 次得到的样本。很容易看出这种抽样是不独立的(为什么?)。这个例子告诉我们，最简单的抽样不一定是简单随机抽样。数理统计书籍从研究简单随机抽样开始，是因为数学上便于更深入地研究。在这样抽取样本下，所求出超几何分布就是统计学中求红球数(统计量)的抽样分布。统计量的抽样分布是统计学中的一个基本问题，因为求得某一统计量的精确抽样分布或者较好的近似，就可以进行计算并且实际进行该统计量的统计推断。

2. 从超几何分布到二项分布

前面我们由实际问题引出了超几何分布，并且讨论了它在估计总体大小以及产品验收方面的应用，但是这个分布不便于计算。我们在这一节中将从逼近超几何分布的角度来导出(或介绍)概率统计中的三个基本分布：二项分布，泊松分布和正态分布。

直观地看，在超几何分布中(见①式)，如果 N 充分大，且 $\frac{M}{N}$ 固定(即从产品检验的例子看，废品率一定)，因而 M 也充分大。那么不论抽取一球是红还是黑，不放回与放回差别不大。于是当 n 相对 N

不大时，我们可以用"放回"模型的分布来"接近"超几何分布。下面便是这一段直观议论的严格表述：

命题 1 设一袋装有 N 个球，其中 M 个红球，$N-M$ 个黑球。从中依次抽取 n 个球，而且每次取出后放回。则抽到的红球数 $X=m$ 的概率

$$P(X=m)=\binom{n}{m}\left(\frac{M}{N}\right)^m\left(1-\frac{M}{N}\right)^{n-m} \qquad ⑦$$

我们用古典概率来解决这个问题(不明显地运用独立的概念)。由排列组合的乘法原理知依次抽取 n 球的方法总数为 N^n，而且所有这种抽取方法都是等可能的。再由排列组合的乘法原理知：在 n 次抽取中，给定的 m 次取到红球(因而其余的 $n-m$ 次取到黑球)的方法数为

$$M^m(N-M)^{n-m}$$

又共有 $\binom{n}{m}$ 种方法确定给定的 m 次，而且每两种给定的 m 次的抽取方法是不同的。所以由加法原理知：依次抽取 n 球，而且每次取出后放回的抽取方法数共有

$$\binom{n}{m}M^m(N-M)^{n-m}$$

所以由古典概率的定义即得①式。

命题 2 按超几何分布的记号 $q(N;\ M,\ n,\ m)$，给定 $\frac{M}{N}=p>0$，则

$$\lim_{N\to\infty} q(N;\ M,\ n,\ m)=\binom{n}{m}p^m(1-p)^{n-m} \qquad ⑧$$

(证明从略)。

命题 1 和命题 2 的意思就是说：当 $\frac{M}{N}=p>0$ 固定，N 充分大

时，超几何分布与放回模型的分布⑦是接近的。

由概率论的初步就知道，⑦、⑧两式的右边就是二项分布。从命题 1 和命题 2 只能导出 p 为有理数的情形。对于任意的 $p \in (0, 1)$，要导出二项分布，就需要引入事件独立的概念和 n 重独立试验模型（或 n 重伯努利试验模型）。

关于独立的概念，我们给出一些注解：

1）我们知道两个事件 A、B 独立是用等式

$$P(A \cap B) = P(A)P(B) \tag{9}$$

定义的。

但是 $n(n > 2)$ 个事件 $A_1, A_2, \cdots, A_n$ 只是满足

$$P(A_1 \cap A_2 \cap \cdots \cap A_n) = P(A_1)P(A_2)\cdots P(A_n) \tag{10}$$

就不能算是独立了。因为由(9)可以导出

$$P(A' \cap B') = P(A')P(B') \tag{11}$$

其中 A' 可以任意取 A 或 A^c（A 的对立事件）。而⑪的四种情况说明事件 A 的发生与否与事件 B 的发生与否无关。但是由⑩并不能导出

$$P(A_1' \cap A_2' \cap \cdots \cap A_n') = P(A_1')P(A_2')\cdots P(A_n') \tag{12}$$

所以只有事件 $A_1, A_2, \cdots, A_n$ 满足⑫式才能认为它们独立。当然⑫式还有其他的等价形式，我们不再多说了。

2）概率论中的独立概念实际是排列组合的乘法原理的类比，后者什么时候适用经常可以根据实际情况比较确切地判断。但是前者则不然，往往只能有一个大致的判断，所以它是一个数学概念。当实际应用需要基于独立假设的结论（例如简单随机抽样的统计量的概率分布）时，就只能根据实际情形判断所进行的抽样是不是独立的，一般不能证明抽样是独立的。

n 次独立试验模型（也称 n 重伯努利试验模型）是：一个由 n 个子试验组成，第 i 次子试验有两个结果：事件 A_i（有时也称为“成

功")及事件 A_i^c("失败"), $P(A_i) = p$, $i = 1, 2, \cdots, n$(因而 $P(A_i^c) = 1 - p$),并且 $A_1, A_2, \cdots, A_n$ 独立。由 n 重伯努利试验很容易导出一般的二项分布。设以 X 表示在 n 次独立试验模型中成功的次数,则 X 的分布是

$$P(X = m) = \binom{n}{m} p^m (1 - p)^{n-m} \qquad ⑬$$

人们称此分布为具有参数 n, p 的二项分布(通常记作 $B(n, p)$),并将⑬的右边的式子记作 $b(m; n, p)$。

⑬式的证明主要是两点(读者可以详细写出来):

1) 由子试验的独立性知:此模型在给定 m 次试验成功(因而 $n - m$ 次失败)的概率是 $p^m (1 - p)^{n-m}$。

2) 指定 m 次试验的方法数为 $\binom{n}{m}$,再由互斥事件之和的概率等于各事件概率之和即得。

既然二项分布是超几何分布的近似(及推广),所以首先有类似于超几何分布的两个应用。用最大似然思想来估计概率 p 并对它进行统计假设检验,以及可以制订产品验收方案。由于类似性,读者可以仿照第一节的办法自己讨论,不再介绍。详情也可参看通常的概率统计教科书。下面我们举一个二项分布的典型应用问题,并说明与此相关的概率应用的有用想法。

例 3 某车间有 10 台电动机功率为 10 千瓦的机床,每台机床工作是独立的,且工作的概率为 $\frac{1}{5}$。若供电部门只提供 50 千瓦的电力给该车间,试求该车间不能正常工作的概率。

解 如果需要开动 5 台以上机床,则该车间就不能正常工作。今以 X 表示该车间需要开动的机床数,则不能正常工作的随机事件是 $\{X \geqslant 6\}$。而上述问题的模型是 $n = 10$, $p = \frac{1}{5}$ 的二项分布。

所以

$$
\begin{aligned}
P(X \geqslant 6) &= 1 - P(X \leqslant 5) \\
&= 1 - \sum_{k=0}^{5} \binom{10}{k} \left(\frac{1}{5}\right)^k \left(1 - \frac{1}{5}\right)^{10-k} \\
&= 1 - 0.993\,63 = 0.006\,37
\end{aligned}
$$

例 4 某电话交换台有 1 000 个用户,在任何时刻各用户是否需要通话是独立的,且每个用户需要通话的概率为$\frac{1}{60}$。问该交换台最少需要多少条线路才能保证各用户在任何时刻同时使用通畅的概率不小于 99%?

将每一用户需要通话与否看成一个子试验,因此用户需要使用电话可以看成是 $p = \frac{1}{60}$ 的 1 000 重独立试验模型。设 X 表示给定时刻需要通话的用户数。按照题意,就是求满足下列不等式的 m,

$$
P(X \leqslant m) = \sum_{k=0}^{m} \binom{1\,000}{k} \left(\frac{1}{60}\right)^k \left(1 - \frac{1}{60}\right)^{1\,000-k} \geqslant 0.99
$$

因为可计算得

m	20	25	26	27	28	30
$P(X \leqslant m)$	0.829 7	0.980 4	0.988 6	0.993 5	0.996 5	0.999 5

所以最少需要 27 条线路。

例 3 说明如果按照该车间的设备,要保证总能正常工作,就需要提供 100 千瓦的电力。由于工人在开动机床的前后,有许多准备或者收尾以及其他工作要做,一台机床实际工作时间不能百分之百,现在经过调查,车间的机床工作大致只占整个时间的五分之一。经过上面的计算知道:只要供应额定电量的一半,就有 99.36%的可能性保证正常工作。既节省了电力,又降低了成本。这个例子实际上是应用概率论的一种广泛而有用的想法具体体现。

现在对多重伯努利试验模型的研究不限于 n(有限整数)重,而且还可以研究(可数)无限重伯努利试验模型。首先要说明的是这种模型的描述需要无穷个事件独立的概念。无穷个事件独立是指其中

任何有限个事件独立。多重伯努利模型及与之相关的论题有很多有趣的结果,还存在一些目前没有解决的问题。我们下面作一些介绍。

3. 一些进一步的例子和问题

(1) 等待时间的分布

考虑如下的问题:设一学生出于好奇,想知道他周围的人中有没有和他生日相同。于是他随机地依次询问他周围人的生日,请问他首次找到同生日的人是第 $m+1$ 个被询问人的概率是多少? 由于各年的天数不一,所以生日是某一天的概率在各年是不一样的。作为近似,我们假定每一年都是 365 天。由排列及古典概率的算法可知(读者自己去算!)所求概率为

$$\frac{(364)^m}{(365)^{m+1}}=\left(1-\frac{1}{365}\right)^m\frac{1}{365}$$

这个例子可以推广如下:

设在多重伯努利试验中,成功的概率是 p,失败的概率是 $q=1-p$,问首次成功在第 $m+1$ 次试验的概率(即试验者等待首次试验成功的时间为 m 的概率)是多少? 不难算出(读者自算!)所求概率是 $q^m p$。这个分布通常称为几何分布。还可以将此问题推广为下列形式:

求首次获得 r 个成功在第 $r+m$ 次试验的概率 $f(m;r,p)$(即试验者等待首次获得第 r 个试验成功的时间为 $r+m-1$ 的概率)是多少? 可以算出(读者自算!)所求概率为

$$f(m;r,p)=\binom{r+m-1}{m}\cdot p^r q^m=\binom{-r}{m}p^r(-q)^m$$

这个分布通常称为负二项分布。这些就是在多重伯努利试验中,两种等待时间的分布。由于在这些问题中,时间是以正整数计算的,通常称为是离散的等待时间分布。

(2) 几何分布、二项分布和负二项分布的关系

为了便于进一步讨论时叙述的方便，我们进一步称模型中的子试验为伯努利试验或两点分布。用算式表示，就是第 i 个子试验用一个取两个值 a、b（前面的定义中是 $a = A$, $b = A^c$ 或 a = 成功，b = 失败，通常是 0, 1 或 -1, 1）的随机变量 Y_i 来表示，其分布为

$$P(Y = a) = p,\ P(Y = b) = q,\ p \in [0,\ 1],\ q = 1 - p$$

于是前面讨论的二项分布、几何分布和负二项分布可以有一个比较一致的说法。

即设 Y_i 所取的两个值分别是 $a = 1$, $b = 0$，且它们之间相互独立，其中每一个的分布都是 $P(Y_i = 1) = p = 1 - P(Y_i = 0)$，而且随机变量 $Y_1 + \cdots + Y_n$ 的分布就是二项分布 $B(n,\ p)$；

$$f(m;\ r,\ p) = P(Y_1 + \cdots + Y_{r+m-1} = r - 1,\ Y_{r+m} = 1)$$

几何分布不过是负二项分布中 $r=1$ 的特例。

(3) 随机游动

我们先来看一看历史上著名而且与上面的讨论有关系的赌徒问题。甲乙二人进行赌博。规定甲胜一局，乙给甲一元；乙胜一局，甲给乙一元。设甲胜一局的概率是 $p(\in (0,\ 1))$，乙胜一局的概率是 $q=1-p$，且每局的胜负相互独立。开始时甲、乙分别有 k, $N-k$ 元，他们一直赌到某人输光为止。问甲赢得全部赌本 N 元的概率。赌博能够永远进行下去的概率有多大？这个问题在很多书中都有讨论，我们只列出结果如下：

设 P_k, Q_k 分别表示甲从 k 元赌本开始直到赢得全部赌本 N 元和输光赌本的概率，从上面征引的文献得知

$$P_k = \begin{cases} \dfrac{1-(q/p)^k}{1-(q/p)^N} & p \neq \dfrac{1}{2} \\ \dfrac{k}{N} & p = \dfrac{1}{2},\ k = 0,\ 1\ \cdots\ N \end{cases} \tag{14}$$

而 Q_k 则表示乙从 $N-k$ 元赌本开始直到赢得全部赌本 N 元的概率。因此为了得到 Q_k 的表达式，只需将上式中的 p、q 互换并将 k

换成 $N-k$ 即可，所以

$$Q_k=\begin{cases}\dfrac{1-(p/q)^{N-k}}{1-(p/q)^{N}} & q\neq\dfrac{1}{2}\\ \dfrac{N-k}{N} & q=\dfrac{1}{2},\ k=0,\ 1\cdots N\end{cases} \tag{15}$$

由 ⑭，⑮ 知，容易算出

$$P_k+Q_k=1,\ k=0,\ 1\cdots N$$

所以赌博永无休止地进行下去的概率为零。赌徒问题在概率论中经常有人提到和介绍的原因可能是由于它是一种随机游动。下面我们对随机游动以及与它的关系作些介绍。用 Y_i 表示取值 -1，$+1$ 的随机变量，它的分布是

$$P(Y_i=1)=p,\ P(Y_i=-1)=q,\ i=0,\ 1,\ \cdots \tag{16}$$

设 X_0 为任一取整数值的随机变量，并令

$$X_n=X_0+Y_1+\cdots+Y_n,\ n=1,\ 2,\ \cdots$$

则称 $\{X_n:\ n=0,\ 1,\ \cdots\}$ 为从 X_0 开始的简单随机游动，是一种特殊的随机过程。也可以将它想象成一个质点从位置 X_0 开始，沿着水平直线逐步移动，每一单位时间按分布律 ⑯ 向右移动一步 ($Y_i=1$) 或向左一步 ($Y_i=-1$)，即向右移动一步的概率是 p，向左移动一步的概率是 q，X_n 就表示质点在直线上时刻 n 的位置，这可能就是随机游动命名的由来。如果 Y_i 表示甲在第 i 局中的输赢，$X_0=k$，那么 X_n 就是第 n 局结束时甲的赌本，所以赌徒问题是一种随机游动。但是它与上述一般的随机游动又有所不同，因为按照赌徒问题的约定，赌博的过程随一方输光而停止，即当 $X_n=N$ 或 0 时，X_{n+1} 就不再存在。此处的 0(N 也一样) 具有一种特殊的性质(在一般随机过程中也有此情况)：过程到此，就被它“吸收”了，不再出现。因此称这种值为过程的吸收壁。赌徒问题看成随机过程是具有两个吸收壁 0，N 的随机游动。在随机游动(以至其他随机过程) 中，还有其他的“壁”。我们就不再进一步介绍了。

简单随机游动是一个离散时间的随机过程，人们对它不是作为孤立的随机变量来研究，而是研究它的整个进程。例如，我们不只是关心 $P(X_n \in [a, b])$ 的大小，而是关心类似于下面的一系列整体性质：

1) 从$(0, N)$中某一点 $X_0 = k$ 出发，质点在到达 N 之前到达0的概率有多大?由赌徒问题知，它就是赌徒输光的概率。

2) 从$(0, N)$ 中某一点 $X_0 = k$ 出发，是否在有限时间内一定碰上 0 或 N (即 $P_k + Q_k$ 是否等于 1)? 这个问题在赌徒问题中已经解决。

3) 从$(0, N)$中某一点 $X_0 = k$ 出发，首次达到 0 或 N 的时间是一个随机变量(想一想!)。那么可以问首次达到 0 或 N 的时间的分布是什么? 或者平均时间有多长?

4) 在一般简单随机游动中，质点从 $X_0 = k \geqslant 0$ 出发，首次到达 0 的概率有多大? 这个问题等同于：求有 k 元赌本的人与一无限富有的人赌博输光的概率。因此可以通过令赌徒问题的输光概率中的 $N \to \infty$ 得到答案。即当 $p \leqslant q$ 时，输光概率是 1；当 $p > q$ 时输光概率是$(qp^{-1})^k$。

上述的简单随机游动是一种在直线上的整数点上运动的随机质点的模型，而且还限定每次运动只能向左或向右移动一步。去掉一限制后就是一般的一维随机游动。还可以进一步讨论在平面或空间(甚至是任意有限维空间)的整数坐标点上的随机游动。有兴趣的读者可以看参考书目。这方面至今还有一些没有解决的问题，国际上仍然有新的学术论文发表。

近年来，由于考虑无序介质(随机介质)背景的情况，提出研究随机环境(或随机介质)下的随机游动问题，其中有一些需要研究的新问题，引起了国际概率论界的注意。

(4) 渗流

渗流理论是以伯努利试验做元件的一种现代概率论理论。近年来，它不但有了迅速的发展，而且有很多没有解决的公开问题。现在我们作一些简单介绍。

渗流模型　设 $d \geqslant 2$ 是一正整数，Z^d 表示 d 维空间中整数坐标点组成的集合。以 Z^d 中相邻两点（即距离为单位的两点）为端点的线段称为边，E^d 表示所有的边的集合。给定一数 $p \in [0, 1]$，对每一边 $e \in E^d$，赋以一个伯努利试验 X_e，其分布为

$$P(X_e = 1) = p = 1 - P(X_e = 0),$$

而且随机变量 X_e，$e \in E^d$ 独立。将随机变量 X_e，$e \in E^d$ 的分布所决定的概率记作 P_p（因为显然这个概率只与 p 有关）。这就是 Z^d 上的边渗流模型。它的实际意义可以理解为：当 $X_e = 1$ 时，边 e 为开，“流”可以通过；当 $X_e = 0$ 时，边 e 为闭，“流”不能通过。

作为无序介质的模型，渗流是具有最少统计相关性的成分组成的最简单模型。它在很多方面引人注意：它容易叙述并且在对随机介质的数量预测方面是现实的；对于那些有意义的更复杂的系统（例如伊辛模型），它是发展数学技巧和洞察力的所在；由它还可以提出一批容易陈述但不容易解决的美丽猜想。有的专家认为渗流理论是无序介质理论的基石，在某些无序物理系统中扮演重要角色，如无序电力网络、铁磁性、果园的流行病、森林中的火灾和薄片集成刻度（Wafer-scale integration，与集成电路的制作有关的工艺）等。

第五节　金融数学例谈

金融数学是现代数学与计算机技术在金融领域中应用所产生的一门新兴学科，它用数学工具研究和发现金融活动的内在规律，并指导金融实践。

金融数学的发展一般认为是从 20 世纪 50 年代开始的。1952 年，美国经济学家、金融学家、诺贝尔经济学奖获得者 H. Markowitz（马科维茨）的论文《资产组合选择》被认为是金融数学的开端。马科维茨因这一对现代金融理论奠基性的贡献，于 1990 年获得了诺贝尔经济学奖。在马科维茨之后，1964～1965 年，另一位 1990 年诺贝尔经济学奖获得者 W. Sharpe（夏普）在投资组合理论的基础上提出了资本资产定价模型（Capital Asset Pricing Model 简称 CAPM）。这个模型研究在单投资周期下，未来收益的概率分布，以及金融资产或金融合同的合理价值。由于证券市场的发展，新的金融产品不断出现，如股票期权在 20 世纪 60 年代到 70 年代发展迅速，如何为这些衍生证券定价成为当时金融界关心的热门问题，经济学家 F. Black（布莱克）和 M. Scholes（斯科尔斯）为解决期权定价做了出色的工作，建立了著名的 Black-Scholes 期权定价公式。斯科尔斯因此在 1997 年与另一位经济学家 R. Merton 获得了诺贝尔经济学奖。至此，新的金融理论——数学金融的框架已经基本形成。

1. 现　　值

货币除了其本身作为商品等价物的价值外，在借贷等流通过程中还有时间价值，这就是利率。

(1) 连续复利

我们知道，利率的计付方法分为单利计息和复利计息。设本金为 C，年利率为 r，期限为 n 年，则单利计息的本利和为

$$S = C(1+nr)$$

复利计息的本利和为

$$S = C(1+r)^n$$

如将一年分成若干个期计息，将会产生怎样的情况呢？设计息的名义年利率仍为 r，一年分为 t 期，则每期利率为 $\frac{r}{t}$，则 n 年共有 nt 期，故 n 年末本利和为

$$S = C\left(1+\frac{r}{t}\right)^{nt},$$

显然，
$$C\left(1+\frac{r}{t}\right)^{nt} > C(1+r)^n$$

这就是说，按相同的名义年利率每年计算 t 次复利比一年只计算一次复利的利息要多，并且可以证明 t 越大，利息越大，但它不会无限增大，实际上

$$\lim_{t\to\infty} C\left(1+\frac{r}{t}\right)^{nt} = Ce^{nr}$$

所以，本金 C 按名义利率 r 无限次计算复利，n 年后本利和为

$$S = Ce^{nr} \qquad ①$$

公式①称为连续复利公式。

必须指出，连续复利公式只是一个理论公式，在实际工作中很少采用，但在作理论分析时则被经常采用，其原因是可以方便地使用分析工具。当 n 不是很大，而 r 又比较小时可作为复利的一种近似估计。

(2) 现值

如果有人问，今天的一万元与明年这个时候的一万元是否相等，

恐怕没有人会回答是。那么明年的这个一万元应该值多少呢？也就是它的现时的价值是多少，这就是货币的现值。

设银行利率为 3%，将 100 元存入银行，一年后可得本利和为 $100(1+3\%)=103$ 元。换一个角度看这个问题，一年后的 103 元，当利率为 3%时，它的现值是

$$\frac{103}{1+3\%}=100(\text{元})$$

这时我们也称 3%为贴现率。

一般地，如果 n 年后有资金 S，贴现率为 r，则它的现值 $PV(S)$ 为

$$PV(S)=S(1+r)^{-n} \quad ②$$

其中 $(1+r)^{-n}$ 称为现值系数。

如果按连续复利计算，则 n 年后资金 S 的现值为

$$PV(S)=Se^{-nr} \quad ③$$

下面是一个用现值评估投资项目的例子。

例 1 某公司有一投资项目，其成本是 500 万元，于年初一次投入，预计今后 4 年内每年年底将为公司带来的净收入分别为 170 万元，180 万元，190 万元，200 万元。如果公司要求这项投资有 15%的投资回报率，问这项投资净收入的现值是多少？投资的净现值是多少？

投资的净现值是指净收入的现值减去投资支出的现值。

解 第一年的净收入的现值为

$$\frac{170}{1+15\%}=147.83(\text{万元})$$

第二年的净收入的现值为

$$\frac{180}{(1+15\%)^2}=136.11(\text{万元})$$

第三年的净收入的现值为

$$\frac{190}{(1+15\%)^3}=124.93(\text{万元})$$

第四年的净收入的现值为

$$\frac{200}{(1+15\%)^4}=114.35(\text{万元})$$

四年净收入的现值总和为 523.22 万元；

这项投资的净现值为 $523.22-500=23.22$ 万元。

这项投资用 15%进行贴现的净现值是正数，说明投资收益率超过 15%，值得采纳。

(3) 股票的内在价值与债券的到期收益率

对股票的评价有各种方法，这里用股票每年股利收入的现值之和来评价其内在价值，所谓内在价值是指股票本身应该具有的价值，而不是它的市场价格。

这种评价方法的根据是，如果你永远持有这个股票(比如你是这个公司的老板，自然要始终持有公司的股票)，那么你逐年从公司获得的股利就是这个股票的价值。

例 2 设 A 公司今年每股股票发放股利 $D_0=1.52$ 元，并且以后每年以 $g=4\%$ 的速度增长，一直到永远，公司股票的期望收益率为 $k=15\%$，求 A 公司股票的内在价值。

解 用股票的期望收益率对公司以后年份的股利进行贴现，然后相加，就可得到它的内在价值 V。

设第 n 年的股利为 D_n，则

$$D_1=D_0(1+g),\ D_2=D_0(1+g)^2,\ \cdots,\ D_n=D_0(1+g)^n,\ \cdots$$

于是

$$V=D_0\cdot\frac{1+g}{k-g} \quad ④$$

将有关数据代入，得

$$V = 1.52 \times \frac{1+4\%}{15\% - 4\%} = 14.37(\text{元})$$

这个股票的内在价值为 14.37 元。

用同样的方法可求现值债券的价值和到期收益率。

设债券的面值为 M,票面利率为 r,每年付息一次,利息 $I=Mr$,债券的年限为 n 年,到期归还面值 M(这种债券称为息票债券)。如果市场利率为 k (一般 $k \neq r$),则有债券价值公式

$$V = \sum_{t=1}^{n} \frac{I}{(1+k)^t} + \frac{M}{(1+k)^n}$$

由计算可知,当市场利率 k 大于票面利率 r 时,债券的价值 V 就低于面值 M;当市场利率 k 小于票面利率 r 时,债券的价值 V 就高于面值 M。

2. 证券组合理论与资本资产定价模型

证券组合理论,是对于有大笔资金的投资者,如何将资金投资于若干个风险证券的最优决策理论。由于证券市场的波动,使得证券、股票的收益变得不确定,这种不确定性就是证券的风险。作为投资者,我们希望能获得较高的收益,同时尽可能地少承担风险。

(1) 证券组合的均值—方差理论

进行证券投资首先要对证券的收益和风险进行度量。对风险证券一般用证券的期望收益率来衡量其收益水平,用收益的方差或标准差来衡量它的风险程度。假定在评判一种证券的优劣时投资者都服从以下两个假设:不满足假设,回避风险假设。

有了这两个假设就可以比较证券的优劣。当两个证券的期望收益率相同时,风险小的就比风险大的要优。同样当两个证券的风险相等时,期望收益率高的就更好一些。

当然,对待风险的态度是因人而异的。有些人为了得到较高的

收益愿意去冒更多的风险，而有些人宁愿收益低一些也不愿意去承担太多的风险。不管投资者对待风险的态度如何，在有相同收益的前提下，总希望风险越小越好，这就是回避风险的愿望。

通常我们用 r 表示证券的收益率，这是一个随机变量，它的数学期望 $E(r)$ 用 $\bar{r}$ 表示，标准差用 $\sigma(r)$ 表示。

由概率论知识，求一个随机变量的期望与方差需要知道该随机变量的分布函数，但对于证券收益率这个随机变量，我们往往不知道它的分布函数。在实际应用中，可用样本均值和样本方差或标准差来代替。设已经知道了随机变量 r 的一组观察值 r_1，r_2，… r_n，则

$$样本均值 \quad \hat{r} = \frac{1}{n} \sum_{i=1}^{n} r_i$$

$$样本方差 \quad \hat{\sigma}^2 = \frac{1}{n-1} \sum_{i=1}^{n} (r_i - \hat{r})^2$$

$$样本标准差 \quad \hat{\sigma} = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (r_i - \hat{r})^2}$$

我们用 σ 作横坐标，$\bar{r}$ 作纵坐标在平面上建立一个直角坐标系，称这个平面为 $(\sigma, \bar{r})$ 平面。这样市场上的任何一个证券均可用 $(\sigma, \bar{r})$ 平面上的一个点来表示。

下面来看 n 个证券的组合。我们尝试用数学方法来解决这样的问题：当收益率水平确定时（即期望收益率为常数），怎样选择在这 n 个证券上的资金投资比例，使组合的风险最小。

设 S_1，S_2… S_n 是 n 个风险证券，它们的期望收益率分别为 $\bar{r}_1$，$\bar{r}_2$… $\bar{r}_n$，风险分别为 σ_1，σ_2… σ_n。证券组合的风险不仅要考虑每种证券收益率的方差或标准差，同时还要涉及两两之间的协方差。由于任何一个企业的景气程度都会受到其他企业的影响，协方差就是企业这种关联性的一种表示。

随机变量 r_i，r_j 的协方差定义为

$$\sigma_{ij} = \mathrm{cov}(r_i, r_j) = E((r_i - \bar{r}_i)(r_j - \bar{r}_j))$$

它刻画了 r_i 与 r_j 之间的一种相关性。

设 S_i，S_j 的收益率 r_i，r_j 的协方差为 σ_{ij}，则我们得到了一个协方差矩阵

$$V = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \cdots & \sigma_{1n} \\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_{n1} & \sigma_{n2} & \cdots & \sigma_{nn} \end{bmatrix}$$

其中 $\sigma_{ij} = \sigma_{ji}$，$\sigma_{ii} = \sigma_i^2$。

如果你有一大笔资金，按照 x_1，$x_2 \cdots x_n$ 的比例，其中 $x_i \geqslant 0$，$x_1 + x_2 + \cdots + x_n = 1$，投资于证券 S_1，$S_2 \cdots S_n$，$x_i \geqslant 0$ 表示不能“卖空”股票 S_i。（“卖空”是一种股票市场的操作机制，就是允许不持有股票 S_i 的投资者卖出 S_i，等 S_i 的价格下跌后再买入 S_i。目前我国证券市场还没有卖空机制），这样就构成了一个证券组合 $p = (x_1, x_2, \cdots, x_n)$。

对组合 $p = (x_1, x_2, \cdots, x_n)$，它的收益率 r_p 是

$$r_p = \sum_{i=1}^{n} x_i p_i$$

期望收益率

$$\bar{r}_p = \sum_{i=1}^{n} x_i \bar{r}_i$$

组合的风险用 σ_p 表示，其中

$$\begin{aligned} \sigma_p^2 &= E((r_p - \bar{r}_p)^2) \\ &= E\{[x_1(r_1 - \bar{r}_1) + x_2(r_2 - \bar{r}_2) + \cdots + x_n(r_n - \bar{r}_n)]^2\} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j E((r_i - \bar{r}_i)(r_j - \bar{r}_j)) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j \sigma_{ij} = X^{-T} V X \end{aligned}$$

$$\sigma_p = \left(\sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j \sigma_{ij} \right)^{\frac{1}{2}} = (X^T V X)^{\frac{1}{2}}$$

其中 $X = p^T$ 是 p 的转置，是列向量。

因为 $x_1 + x_2 + \cdots + x_n = 1$，上述方程是含有 $n-1$ 个参数的参数方程（假定参数是 $x_1, x_2, \cdots, x_{n-1}$）。对所有可能的 $x_1, x_2 \cdots x_{n-1}$，相应的$(\sigma, \bar{r})$得到平面上的一个点集。对点集中的任何点 P，都存在证券 $S_1, S_2 \cdots S_n$ 的一个组合 $p = (x_1, x_2, \cdots, x_n)$，由这个组合得到的 σ_p 和$\bar{r}_p$ 正好就是 P 点的坐标。而在集合外的任何点，都无法找到 $S_1, S_2 \cdots S_n$ 的组合与之对应。因此我们就称这个集合为证券 $S_1, S_2, \cdots, S_n$ 的可行集。容易证明，当 $n = 2$ 时，可行集是一条曲线；$n \geqslant 3$ 时，可行集是一平面区域（如图 3.5.1 与3.5.2）。

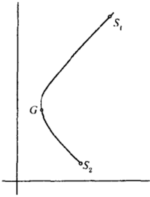


图 3.5.1 两个证券的可行集

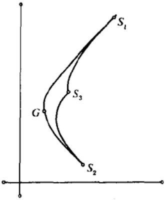


图 3.5.2 三个证券的可行集

注意在可行集（图 3.5.2）中，弧 S_1S_2 称为可行集的前沿，而弧 S_1G 称为有效前沿。前沿是对确定的期望收益率水平有最小的方差或标准差的组合，有效前沿是对确定的期望收益率水平有最小方差，同时对确定的方差水平有最大的期望收益率的组合。有效前沿是前沿的一个子集，前沿上的点表示的组合也称为最小方差组合。

根据前沿的定义，求前沿就是在一定的期望收益率下，求风险最小的组合 p。这样就归结为下列二次规划的解：

目标函数为

$$\sigma_p^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j \sigma_{ij} = X^{-T}VX$$

约束条件为

$$\begin{cases} \sum_{i=1}^{n} x_i = X^T I = 1 \\ \sum_{i=1}^{n} x_i \bar{r}_i = X^T \bar{R} = \bar{r}_p \end{cases}$$

这里 $$I = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix},\ \bar{R} = \begin{bmatrix} \bar{r}_1 \\ \bar{r}_2 \\ \vdots \\ \bar{r}_n \end{bmatrix},\ X = p^T = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

可以证明,证券组合的前沿是双曲线的一部分。在这条曲线上有一个特殊点 G(见图 3.5.2),它的方差在所有可行组合中最小。这个点称为整体最小方差组合,与其对应的坐标为

$$\bar{r}_g = \frac{b}{c},\ \sigma_g^2 = \frac{1}{c}$$

对应的组合是

$$p_g^T = X_g = \frac{V^{-1}I}{c}$$

其中

$$a = \bar{R}^T V^{-1} \bar{R},\ b = \bar{R}^T V^{-1} I,\ c = I^T V^{-1} I$$

关于最小方差组合,还有以下的定理

定理 (两个基金分离定理)设 X_a, X_b 是最小方差组合,则任何一个最小方差组合 X 均可唯一地表示成 X_a 与 X_b 的线性组合:

$$X = \alpha X_a + (1-\alpha) X_b \qquad ⑤$$

特别地,当 X_a, X_b 是有效前沿,$0 \leqslant \alpha \leqslant 1$ 时,X 也是有效前沿组合。

从定理看出，所有的最小方差组合都可以由两个不同的最小方差组合 X_a 与 X_b 生成，通常称 X_a 与 X_b 为“共同基金”，因此公式⑤称为两个基金的分离定理。有了这个定理，不管投资者对待风险的态度如何，通过购买以上两个基金的组合就可以满足要求。这就是基金分离定理的重要之处。

(2) 具有无风险资产的均值——方差证券组合理论

当市场上存在无风险证券(通常指三个月期的国债，在没有三个月期国债时，可以用三个月期的银行存款代替)时，证券组合的问题就发生了变化，投资者在风险证券上的投资不一定是他的全部资产，他可以用一部分资金购买国债或储蓄，也可以负债购买风险证券。另外在衡量风险证券的投资收益率时就有了比较，超过无风险证券收益率部分才是投资者所追求的。因此，最小方差组合问题可以表述成下列的优化问题：

设无风险资产 F 的收益率为 r_f，S_1，$S_2 \cdots S_n$ 的期望收益率为 $\overline{r}_1$，$\overline{r}_2 \cdots \overline{r}_n$，投资于证券 F，S_1，$S_2 \cdots S_n$ 的组合

$$p = (y,\ x_1,\ x_2 \cdots x_n)$$

并且

$$y + \sum_{i=1}^{n} x_i = 1,$$

这里 y 和 x_i 分别是投资于无风险证券 F 和 S_i 的资金比例；以 $\hat{r}_i = \overline{r}_i - r_f$ 表示 S_i 的期望超额收益率，则组合的期望超额收益率 $\hat{r}_p$ 为

$$\hat{r}_p = \sum_{i=1}^{n} x_i \hat{r}_i = \sum_{i=1}^{n} x_i (\overline{r}_i - r_f) \qquad ⑥$$

这样具有无风险证券的最小方差证券组合问题可表述为下列优化问题：

$$\min \sigma_p^2 = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j \sigma_{ij} \qquad ⑦$$

限制条件

$$\sum_{i=1}^{n} x_i \hat{r}_i = \hat{r}_p \qquad ⑧$$

与前一小节类似,用 Lagrange 乘数法可以得到含无风险证券组合的有效前沿。这里我们省略求解过程,而来讨论它的几何意义。

见图 3.5.3,在$(\sigma, \bar{r})$面上,曲线 C 是风险证券 $S_1, S_2 \cdots S_n$ 的有效前沿,F 是无风险证券。过 F 引一直线与 C 相切,切点为 M。将 M 看成一个“新”的证券,则线段 FM 就是证券 F 与 M 的可行集(由于 F 是无风险证券,它的方差以及与 M 的协方差均为 0,因此确定可行集是一直线段),当然也是证券 $F, S_1, S_2 \cdots S_n$ 的可行集。同时,不难看出,$F, S_1, S_2 \cdots S_n$ 的可行组合所对应的点都在 FM 的东南方,西北方都不是可行组合,根据有效前沿的定义,FM 就是含有无风险证券的组合 $F, S_1, S_2 \cdots S_n$ 的有效前沿。

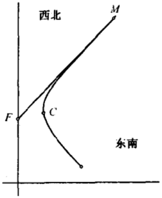


图 3.5.3

有意思的是,$F, S_1, S_2 \cdots S_n$ 的有效前沿直线与纯风险证券 $S_1, S_2 \cdots S_n$ 组合的有效前沿双曲线有一个切点,这个切点称为切点组合。很明显,当投资于无风险证券的资金为 0,即 $y=0$ 时,对应切点组合 M。这个“切点组合”与投资者个人的对风险的态度无关。也就是说,不管投资者对待风险的态度如何,只要他想得到最优投资组合,就必须选择 M 与 F 进行组合,差别只是在于投资于 F 资金的比例的多少,喜好风险的投资者可以少投或不投资金于无风险证券 F,而不喜好风险的投资者则多投资金于 F。因此,所有的最小方差组合都可以表示为无风险证券与切点组合的线性组合,这个性质称为货币分离定理。

下面我们就两个风险证券于无风险证券的组合举一个例子来说明这个理论。

例 1 设市场上有两种风险证券 S_1, S_2,它们的期望收益率和风险分别为

$$\bar{r}_1 = 6.10\%,\ \sigma_1 = 8\%,\ \bar{r}_2 = 10.20\%,\ \sigma_2 = 15.1\%$$

S_1，S_2 的协方差 $\sigma_{12} = 0.4\%$，无风险证券 F 的收益率为 4%。

首先，证券 S_1，S_2 的期望超额收益率分别为 2.1%和 6.2%，则⑦式，⑧式为

$$\sigma_p^2 = x_1^2\sigma_1^2 + 2x_1x_2\sigma_{12} + x_2^2\sigma_2^2$$
$$= 0.006\,4x_1^2 + 0.008x_1x_2 + 0.022\,8x_2^2$$
$$0.021x_1 + 0.062x_2 = \hat{r}_p$$

作 Lagrange 函数

$$L = 0.006\,4x_1^2 + 0.008x_1x_2 + 0.022\,8x_2^2$$
$$-\lambda(0.021x_1 + 0.062x_2 - \hat{r}_p)$$

对 x_1，x_2 求偏导

$$\frac{\partial L}{\partial x_1} = 0.012\,8x_1 + 0.008x_2 - 0.021\lambda$$

$$\frac{\partial L}{\partial x_2} = 0.008x_1 + 0.045\,6x_2 - 0.062\lambda$$

令偏导为 0，解得

$$x_1 \approx 0.888\,239\lambda,\ x_2 \approx 1.203\,818\lambda$$

切点组合就是当 $y = 0$ 时，x_1，x_2 的值，因此只要令 $x_1 + x_2 = 1$ 得

$$x_1 \approx 0.424\,6,\ x_2 \approx 0.575\,4$$

切点组合 $p_m = (0.424\,6,\ 0.575\,4)$。

因此，切点组合对应的期望收益率及方差、标准差为

$$\bar{r}_m = 0.424\,6 \times 6.1\% + 0.575\,4 \times 10.2\% = 8.46\%$$

$$\sigma_m^2 = 0.424\,6^2 \times 0.006\,4 + 2 \times 0.424\,6 \times 0.575\,4 \times 0.004$$
$$+ 0.575\,4^2 \times 0.022\,8 = 0.010\,66$$

$$\sigma_m = 10.32\%$$

有效前沿是连接点$(0, r_f)$与点$(\sigma_m, \bar{r}_m)$的线段

$$\bar{r}_p = 0.04 + 0.431\,8\sigma_p$$

以上是两个风险证券的例子，对于 n 个风险证券，求解的基本步骤是一样的，只是需要解一个 n 元线性方程组。

3. 期权的定价——Black-Scholes 公式

(1) 期权的背景和概念

随着金融市场的日益发展，各种衍生证券不断出现，期权(Option)就是其中最具代表性的一种。

期权是一种将来的选择权。期权持有人有在约定期限以敲定价格向期权出售者购买(这类期权称为看涨期权)或者出售(这类期权称为看跌期权)某种资产的权利，并且期权持有人还可以选择执行或者不执行这种权利。期权的执行也有两种形式，只能在期满日执行的称为欧式期权，可以在期满日及之前的任何一天执行的称为美式期权。例如，某股票的现时价格为 $S = 53$ 元，它的年波动率为 $\sigma = 20\%$，市场上无风险证券的年收益率为 $r = 10\%$，如果你希望拥有一个在六个月后 (即半年，$T = 0.5$) 以敲定价格 $X = 50$ 元购买该股票的期权，问你应该付多少钱？这就是一个欧式看涨期权的问题。

由于这种权利对持有人是绝对优惠，他应该为此付出代价，不然就不会有人出售期权，这就是期权的价格。期权价格是一种未定权益的价格，它的定价长期以来一直是依靠经验进行的。到 20 世纪 70 年代，F. Black 与 M. Scholes 在假定标的资产(指金融市场上的商品，如股票、债券、外汇、股票指数等)的价格波动符合几何布朗运动时，推导出了期权价格变化必须满足的微分方程，从而得到了第一个精确的期权定价模型，引起了各界的巨大反响。

(2) Black-Scholes 方程

1) 实例分析

我们先仔细分析一下期权价格的确定过程。设股票的现价为 S，由于股票价格的波动率，到了 T 时刻价格可能上扬到 Su，也可能下跌至 Sd。为简单计，假定涨跌幅均为 10%，则 $u = 1.1$，$d = 0.9$，到时期权的价格会怎样呢？显然，当股票价格上扬到 58.3 时，你会执行期权，以敲定价格 50 元买入股票，然后以 58.3 元的价格卖出。因此这时的期权价格应该为

$$V_u = Su - X = 58.3 - 50 = 8.3$$

而当股票价格跌到 47.7 元时，你一定选择放弃执行期权，这时的期权价格应为

$$V_d = 0$$

总之到期满日 T 时，期权价格应该为

$$V_T = \max(S_T - X,\ 0)$$

对期权而言定价问题是一个反向的问题，即当知道了时刻 T 时的期权价值 V_T，求初始时刻的值。

Black-Scholes 期权定价模型的基本思想是套期保值，“套期保值”是一种为了避免风险而采取的投资组合（在英语中投资组合和证券组合都是用 portfolio 这个词，我们在此也不加区别）的策略。假定现在投资者以价格 V 卖出一份股票期权，再买入 a 份这种股票，则组合的价格为

$$\Pi = aS - V \qquad ⑨$$

a 是待定的系数。作这个组合的目的是使 Π 没有风险，从而可以获得无风险利率。于是在期权期满日，组合的价值应该是无风险利率

$$\Pi_T = \rho\Pi \qquad ⑩$$

其中 $\rho = e^{rT}$ 是无风险利率 r 在 T 时刻的连续复利。

同时，从期权的价值考虑，在时刻 T，由⑩式得

$$\Pi_T = aS_T - V_T = \begin{cases} aSu - V_u \\ aSd - V_d \end{cases} \tag{⑪}$$

根据组合无风险,应该有

$$aSu - V_u = aSd - V_d$$

$$a = \frac{V_u - V_d}{S(u-d)}$$

代入⑪,得到

$$\Pi_T = \frac{d}{u-d}V_u - \frac{u}{u-d}V_d \tag{⑫}$$

将⑨,⑫代入⑩,得

$$V = \frac{1}{\rho}\left[\frac{\rho - d}{u-d}V_u + \frac{u-\rho}{u-d}V_d\right] = \frac{1}{\rho}[pV_u + (1-p)V_d] \tag{⑬}$$

这里 $p = \dfrac{\rho - d}{u-d}$, 显然,$p$ 正是股票上涨的概率,(13)式中方括号内恰好是期权价格在时刻 T 时的期望。这样(13)式就变成

$$V = \frac{1}{\rho}E(V_T)$$

用已知数据代入,容易得到

$$\rho = e^{0.1\times 0.5} \approx 1.051,\ u = 1.1,\ d = 0.9,\ p \approx 0.755$$

从而由(13)可以求出

$$V \approx 5.962$$

这是一个十分粗略的例子,许多假设也过于简单,但是套期保值的思想在期权定价理论中的作用已十分明显。

2) Black-Scholes 方程

有了前面的准备,下面简单讨论连续情形下的期权定价问题,基本思想是一样的。

设股票价格的变化遵从几何布朗运动(布朗运动是生物学家布朗在观察植物花粉在水中运动时发现的),即当 S 为股价时,有

$$\frac{dS}{S} = \mu dt + \sigma dz \tag{⑭}$$

这里 μ 是股票的预期收益率,σ 是股票的波动率。由于 S 是随机变量,上式不是通常意义下的微分,其右端的第一项是确定项,而第二项则是随机微分项,可表示为

$$\sigma dz = \varepsilon\sqrt{dt}$$

这里 ε 是服从标准正态分布的随机变量,即 $\varepsilon \sim N(0,\ 1)$。将⑭式表示为离散形式,得

$$\frac{\Delta S}{S} = \mu\Delta t + \sigma\varepsilon\sqrt{\Delta t} \tag{⑮}$$

这说明在 Δt 时刻之后,股票的收益率 $\frac{\Delta S}{S}$ 是随机变量 ε 的线性函数,因此仍为一个服从正态分布的随机变量,并且它的期望是 $\mu\Delta t$,方差是 $\sigma^2\Delta t$,即:

$$\frac{\Delta S}{S} \sim N(\mu\Delta t,\ \sigma\sqrt{\Delta t})。$$

这就对股票的预期收益率与股价的波动率有了一个较为确切的认识。

如同⑨式作套期保值组合,则组合 Π 在单位时间内的收益率应为无风险利率 r。于是有

$$\frac{d\Pi}{\Pi} = r dt \tag{⑯}$$

用⑨式代入得

$$dV - a dS = r\Pi dt$$

为确定常数 a,引用随机分析的 Ito 公式

$$dV = \left(\frac{\partial V}{\partial t} + \mu S \frac{\partial V}{\partial S} + \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 V}{\partial S^2}\right)dt + \sigma S \frac{\partial V}{\partial S}dz$$

整理后得到

$$\left(\frac{\partial V}{\partial t} + \mu S \frac{\partial V}{\partial S} + \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 V}{\partial S^2} - a\mu S\right)dt + \left(\sigma S \frac{\partial V}{\partial S} - a\sigma S\right)dz$$
$$= (rV - arS)dt (= r\Pi dt = d\Pi)。 \quad ⑰$$

上式右端是 $d\Pi$，而 Π 是无风险的，因此随机微分项为零，即有

$$\sigma S \frac{\partial V}{\partial S} - a\sigma S = 0$$

于是

$$a = \frac{\partial V}{\partial S}$$

将⑰代入⑯，就得到了期权价值 V 应该满足的 Black-Scholes公式

$$\frac{\partial V}{\partial t} + \frac{1}{2}\sigma^2 S^2 \frac{\partial^2 V}{\partial S^2} + rS \frac{\partial V}{\partial S} - rV = 0 \quad ⑱$$

注意到在公式⑱中并不出现股票的预期收益率 μ，这就是说期权定价与 μ 无关。这使我们可以假定股票及其衍生物的预期收益率都是无风险利率 r。这种假设称为风险中性假设。

第六节　小波分析及其应用

信号是信息的载体，信息的传播离不开信号。电话、收音机、收录机传播声信号，电视机传播图像信号与声信号，多媒体技术使多种媒体传播的信号统一起来处理。

1. 信号的数学表示

什么是信号？在数学上怎样表示这些信号？从数学观点来看，信号有两种解释和表示方式。

连续时间信号可看作一个以时间为自变量的函数。采样信号可看作一个数字序列(时间序列)，如下列的数列表示一个信号。(由于实际数据太长，这里仅取前 70 个)。

−1.297 7	−4.100 0	1.914 8	2.623 1	−1.900 6	4.572 7
3.930 8	−0.254 9	0.618 6	0.245 1	−0.560 1	2.456 1
−1.401 7	6.691 6	−0.772 5	−0.658 2	1.661 5	−1.582 2
−1.825 8	−3.393 9	0.883 2	−3.111 7	3.681 8	6.630 8
−0.536 5	3.574 0	4.125 3	−4.923 2	−4.686 2	1.434 7
−1.199 7	2.348 8	2.810 1	2.277 8	3.507 5	1.005 8
2.033 7	−5.367 4	−1.598 2	−1.367 0	−4.812 3	1.668 7
−1.630 6	6.005 5	−0.876 4	2.586 2	1.021 2	−2.907 7
−6.875 3	−0.456 3	−3.031 9	2.122 2	1.886 5	5.219 3
1.410 6	−2.930 8	−0.397 8	−4.787 4	−1.597 4	−1.041 5
0.000 1	−0.056 8	4.823 9	−3.861 9	2.823 4	3.686 9
2.556 1	1.591 5	−0.242 3	1.752 5		

以序列下标(实际上表示时间)为横坐标,以数列中项的数值为纵坐标作图,并把各点相连结得图 3.6.1,于是平面图像信号可以看作取矩阵值的函数。从上面的数列很难得出信号的整体形象,而图 3.6.1 可以看到信号变化的整体态势,信号的幅值随时间不规则地变化。

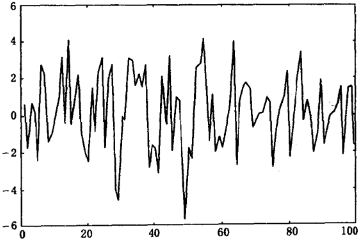


图 3.6.1

那么这个信号有没有规律?它表示什么信号?从图 3.6.1 无法回答这些问题。因此需要换个角度来看信号。

信号可看作不同频率正弦信号的叠加。把一个信号分解成若干频率成分,可以用一个频谱图来表示。例如上面信号的频谱图如图 3.6.2 所示。

在图 3.6.2 中,横坐标 50 和 100 处有两个突出尖峰,它们表示图 3.6.1 所示信号主要是由 50 Hz 的正弦波、100 Hz 的正弦波叠加而成,横坐标其余处峰值很小的波表示随机噪声。这就是说,由数列或图 3.6.1 所示信号可以表示为

$$y(t)=\sin(2\pi\times 50t)+\sin(2\pi\times 100t)+\text{噪声}$$

如果设 50 Hz 的信号是由航空母舰发出的,100 Hz 的信号是由核潜艇发出的,那么在图 3.6.1 中看起来毫无规则的信号竟是一艘航空母舰和一艘核潜艇来犯的信号。

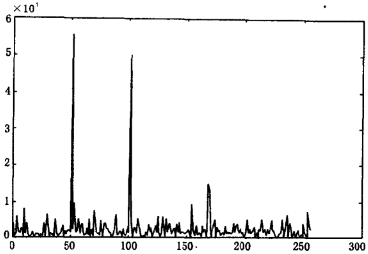


图 3.6.2

由此可见信号频域表示的重要性。事实上，质谱仪利用频谱分析有无有害的化学物质。用声纳和频谱分析来发现鱼群，其原理是一样的。

图 3.6.1 中横坐标表示时间 t，纵坐标表示信号的幅值。图 3.6.2中横坐标表示频率 f，纵坐标表示该频率成分的大小。

由数据求其频谱要使用傅里叶(Fourier)分析。

2. 傅里叶级数

傅里叶(Joseph Fourier 1768—1830)是一位与拿破仑同时代的法国数学家。他曾经是拿破仑的御用科学家，随军远征埃及，对古埃及文化研究作出过贡献。1807 年他提出了下列形式的级数：

$$\phi(x)=\begin{cases}1 & x\in[0,\ 1)\\ 0 & x\notin[0,\ 1)\end{cases}$$

$$a_0+\sum_{k=1}^{\infty}a_k\cos kx+b_k\sin kx \qquad ①$$

如果只取有限多项的部分和，则称为三角多项式。其中 a_k，b_k 都是实数，称为傅里叶系数。其实这样的级数最早出现在欧拉给出的公式中：

$$\frac{x}{2} = \sin x - \frac{1}{2}\sin 2x + \frac{1}{3}\sin 3x - \cdots \qquad ②$$

但在数学史上并没有把①称为欧拉级数，而称为傅里叶级数。这是因为傅里叶对①的研究更为系统，影响也大些。

所谓欧拉等式指

$$e^{i\theta} = \cos\theta + \mathrm{i}\sin\theta。$$

该式可改写为

$$\cos kx = (e^{\mathrm{i}kx} + e^{-\mathrm{i}kx})/2$$

$$\sin kx = (e^{\mathrm{i}kx} - e^{-\mathrm{i}kx})/2\mathrm{i}$$

其中 i 是虚数单位。把上面的公式代入①经整理可得

$$\sum_{k=-\infty}^{\infty} C_k e^{\mathrm{i}kx} \qquad ③$$

其中

$$C_0 = a_0,\ C_k = (a_k - \mathrm{i}b_k)/2,\ C_{-k} = (a_k + \mathrm{i}b_k)/2。$$

C_k 的范数表示 $e^{\mathrm{i}kx}$ 成分的多少。

在 Matlab 中作序列 y_n 的傅里叶变换可以用函数 fft，而序列元素的个数应取 2 的正整数幂。

fft(y)是向量 y 的离散傅里叶变换。对于长度为 N 的向量，其傅里叶变换是

$$Y(f) = C_f = \sum_{n=1}^{N} y_n e^{-\mathrm{i}\cdot 2\pi(f-1)(n-1)/N},\ 1 \leqslant f \leqslant N \qquad ④$$

傅里叶逆变换是

$$y_n = \frac{1}{N}\sum_{k=1}^{N} Y(k)\cdot e^{i\cdot 2\pi(k-1)(n-1)/N},\ 1 \leqslant n \leqslant N \qquad ⑤$$

用下列语句可以产生时域信号,

```
t = 1:512;
y = sin(2 * pi * 50 * t/512) + sin(2 * pi * 100 * t/512) + 2 * randn
(1,512);
```

用"plot(y(1:100))"语句可产生图 3.6.1 那样的图象,为了让图看起来清晰,只画前 100 点的连结图。

用下列语句可进行傅里叶变换并画出其频谱图。

```
Y = fft(y);
Z = Y. * conj(Y);
plot(Z(1:256))
```

这里还要说明一点:图 3.6.1 是频率 $f = 50,100$ 的两个正弦波与噪声 2 * randn(·)的叠加。④中的 f 在信号分析中常换成 ω,称为角频率,它与 f 有如下关系:

$$\omega = 2\pi f$$

3. 小波分析为什么走红

虽然傅里叶分析能告诉人们信号中的频率成分,但不能告诉人们具有那个频率的波产生于什么时刻。从④可以看出 y_n 的傅里叶变换 $Y(f)$只是频率 f 的函数而不再是时间 n 的函数。

如果有一种变换既告诉人们信号中的频率成分又告诉人们频率成分发生的时间,那么对于敌舰信号的分析是十分有益的。

语言信号不仅依赖于频率而且与频率发生的时间有关,因此语音识别也需要这种既能表达频率又能表达时间的变换。小波分析是一种时频域的分析,满足了实际需要,因而在 20 世纪 80 年代

中期开始获得蓬勃发展，在信号压缩（compression）中取得了巨大的成功。

在信号传输中，信号的压缩和复原（reconstruction）是十分重要的技术。一张照片是 256×256 个像素灰度值组成的矩阵，存贮或传输要占用 65 536 个单元，电视每秒需要几十个画面，而一个光缆要传几十个电视台的节目，可见传输量之大。因此如能压缩数据量，接收后又能很好复原就显得十分重要。

女数学家道贝契斯（Daubechies）利用小波把美国洛杉矶警局的犯人指纹档案存贮量压缩到原先存贮量的二十分之一，消息传出轰动了信号处理界。

小波分析已成功地应用于地震勘探的数据分析和寻找可能贮油的地质结构。法国的 Meyer 和我国安徽大学的李世雄都用此法。

小波可用于去除信号中的噪声干扰，这方面我们有成功的项目。

小波级数实质上是一种展开式。用小波级数来逼近非线性函数可以达到很高的精度。因此小波已成为微分方程数值解的有力工具。

小波不仅有广泛的应用，而且有坚实的理论，这是学科发展的必备条件。

由于上述理由，小波研究的走红就是必然的了。

4. 数据压缩和信号恢复

为了讲清数据压缩的概念，我们介绍一下用代数方法进行数据压缩的方法。假定原始信号是一幅渔网图。它是由 $33\times33=1\,089$ 个数据排成的一个矩阵 z。这个矩阵中的每一个元素表示在该位置上纵坐标的高度，把不同高度的点用网格图连成的形似渔网三维图形（见 3.6.3）。

假设我们要传输这个图象信号，就把矩阵 z 进行奇异值分解。

用语句： [U, S, V] = SVD(z);

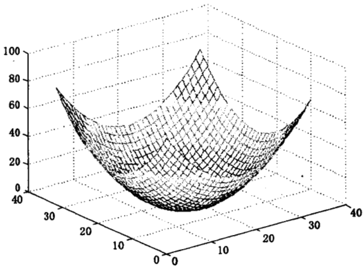


图 3.6.3 原始信号

其中 U 和 V 都是 33×33 的矩阵,而 S 是一个对角阵,只有 6 个元素不为 0:

$$S=\begin{pmatrix} 1.3860 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.3005 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.0218 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.0041 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.0011 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.0001 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

这里

$$z=USV^{\tau}=\sum_{i=1}^{33}\sigma_i\mu_i\nu_i^{\tau} \qquad ⑥$$

其中 μ_i 表示 U 中第 i 列,ν_i 表示 V 中第 i 列,σ_i 为非零对角元。由于 σ_5, σ_6 很小,近似为零,$\sigma_7=\cdots=\sigma_{33}=0$,因此只取前四项,即

$$z=\sum_{i=1}^{4}\sigma_i\mu_i\nu_i^{\tau} \qquad ⑦$$

所以只要保存 U 中第 1 至 4 列，V 中第 1 至 4 列和 σ_1，σ_2，σ_3，σ_4，就可以恢复。

用 Matlab 语句：

```
uu = U(1:33, 1:4);
vv = V(1:33, 1:4);
ss = S(1:4, 1:4);
```

那么就能恢复成

```
zz = uu * ss * vv';
mesh(zz)
```

恢复后的图象如图 3.6.4。

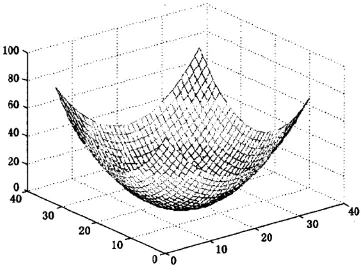


图 3.6.4　由压缩信号恢复的图

将图 3.6.3 和图 3.6.4 相比较，人眼根本不能分辨它们的差别。因此在一定精度要求下，我们不必传输 z 矩阵 ($33 \times 33 = 1\,089$ 个) 的数据，而只要传递 $4 \times 33 + 4 \times 33 + 4 = 268$ 个数据，即只要传送 $\mu\mu$，$\nu\nu$ 和 σ_1，σ_2，σ_3，σ_4 即可。其压缩比为

$$\text{Ratio} = \frac{\text{原数据量}}{\text{压缩后传输的数据量}} = \frac{1\,089}{268} = 4.06 \qquad ⑧$$

这样做大大减少了该图象的传递时间。

为了表述简单，下面考虑用小波分析的方法进行一维信号的压缩。

设 $y(t)$为一批信号，现采得 200 点 $y(t_1)$, $y(t_2)$, …, $y(t_{200})$。这里 $t_1 < t_2 < \cdots < t_{200}$。

墨西哥草帽的小波(母小波)为：

$$\Psi(t) = \frac{2}{\sqrt{3}}\pi^{-\frac{1}{4}}(1-t^2)e^{-\frac{t^2}{2}} \qquad ⑨$$

若 $t_{200} - t_1 = 2\pi$，小波的基取作

$$\Psi_k(t) = \Psi\left(t - \frac{2k\pi}{N}\right) \qquad ⑩$$

对于给定的 m(表示精度)，对信号

$$y(t) = \sum_{k=1}^{N} C_k \Psi_k(t) \qquad ⑪$$

作目标函数

$$J(C_1, \cdots, C_n) = \sum_{t=t_1}^{t_n}\left[y(t) - \sum_{k=1}^{N} C_k \Psi_k(t)\right]^2 \qquad ⑫$$

令

$$\theta = (C_1, \cdots, C_N)^\tau = (\theta_1, \cdots, \theta_N)^\tau$$

$$\Phi(t) = (\Psi_1, \Psi_2, \cdots, \Psi_N(t))^\tau \qquad ⑬$$

则⑫可写成

$$J(\theta) = \sum_{t=t_1}^{t_n}[y(t) - \theta^\tau \Phi(t)]^2$$

再令

$$E = \begin{bmatrix} y(t_1) - \theta^\tau \Phi(t_1) \\ y(t_2) - \theta^\tau \Phi(t_2) \\ \vdots \\ y(t_n) - \theta^\tau \Phi(t_n) \end{bmatrix}$$

$$= Y - \begin{bmatrix} \Psi_1(t_1) & \Psi_2(t_1) & \cdots & \Psi_N(t_1) \\ \Psi_1(t_2) & \Psi_2(t_2) & \cdots & \Psi_N(t_2) \\ \vdots & & & \\ \Psi_1(t_n) & \Psi_2(t_n) & \cdots & \Psi_N(t_n) \end{bmatrix} \theta$$

$$\Phi = \begin{bmatrix} \Psi_1(t_1) & \Psi_2(t_1) & \cdots & \Psi_N(t_1) \\ \Psi_1(t_2) & \Psi_2(t_2) & \cdots & \Psi_N(t_2) \\ \vdots & & & \\ \Psi_1(t_n) & \Psi_2(t_n) & \cdots & \Psi_N(t_n) \end{bmatrix} \quad Y = \begin{bmatrix} y(t_1) \\ y(t_2) \\ \vdots \\ y(t_n) \end{bmatrix}$$

则

$$E = Y - \Phi\theta$$

所以

$$\begin{aligned} J(\theta) &= (Y - \Phi\theta)^{\tau}(Y - \Phi\theta) \\ &= Y^{\tau}Y - Y^{\tau}\Phi\theta - \theta^{\tau}\Phi^{\tau}Y + \theta^{\tau}\Phi^{\tau}\Phi\theta \\ &= [\theta - (\Phi^{\tau}\Phi)^{-1}\Phi^{\tau}Y]^{\tau}\Phi^{\tau}\Phi[\theta - (\Phi^{\tau}\Phi)^{-1}\Phi^{\tau}Y] \\ &\quad + Y^{\tau}Y - Y^{\tau}\Phi(\Phi^{\tau}\Phi)^{-1}\Phi^{\tau}Y \end{aligned}$$

等式左边的第一项是平方和，令其等于零，$J(\theta)$达到最小值，因此 θ 的最小二乘估计(即使得目标函数 $J(\theta)$达到最小值的 θ)为

$$\hat{\theta} = (\Phi^{\tau}\Phi)^{-1}\Phi^{\tau}Y$$

其中 Y 向量是原始信号的离散值。

图 3.6.5 中的 y 假定是要传送的信号。利用小波展开压缩，并不需要传送所有的 y 值，而只要传送由下列程序求出展开式系数就行了。为求 Φ 矩阵，编写下列子程序：

```
function f = mexicohat (n, bign)
for t = 1:n
  for k = 1:bign
```

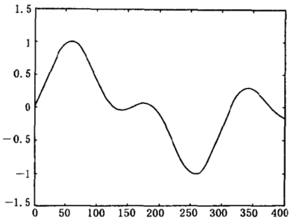


图 3.6.5 原始信号

```
        x = (t − 1) * 2/n * pi − k/bign * 2 * pi;
        f(t, k)=2/3^(1/2) * pi^(−1/4) * (1−x^2) * exp(−x^2/2);
    end
end
```

然后在 Matlab 命令窗口下执行：

```
f = mexicohat(400, 12);
y = y';
c = inv(f' * f) * f' * y;
```

用下列语句求模型值：

```
ym = f * c;
plot(ym)
```

得恢复后的图象(图 3.6.6)。

如果给定了展开式中的基函数的形式，那么只要输送 12 个 θ 值就可以恢复原图象，压缩比达到：

$$\text{Ratio} = \frac{400}{12} = 33.33$$

用奇异值分解压缩数据是一种有效的方法。然而，用小波方法进行数据压缩和信号恢复，其压缩比远大于用奇异值分解进行数据

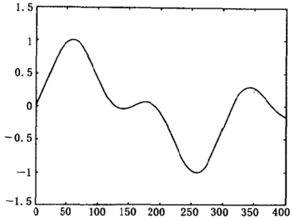


图 3.6.6　恢复后的信号

压缩和信号恢复的压缩比。由此可见，用小波进行数据压缩是一种比较好的方法。但是，如何选择小波基和用多少项进行数据压缩值得进一步研究。

§5　方箱函数和哈尔小波

为了让学生理解小波的特性，下面介绍一种最简单的小波，哈尔(Haar)小波。为了讲哈尔小波，要先从方箱函数说起。所谓方箱函数指下列函数：

$$\phi(x) = \begin{cases} 1 & x \in [0,\ 1) \\ 0 & x \notin [0,\ 1) \end{cases}$$

其图象如3.6.7。

实际过横坐标1的垂直线段是没有的，这样画仅仅为了看起来清楚一些。定义下列函数：

$$\text{supp}\,\phi(x) = \{x \mid \forall \varepsilon > 0,\ \exists\, y \in (x-\varepsilon,\ x+\varepsilon):\phi(y) \neq 0\} = [0,\ 1]$$

定义表明 supp $\phi(x)$是使得函数 $\phi(x)$不等于零的点集加上其极限点所构成的集合，它称为函数 $\phi(x)$ 的支撑(support)。当

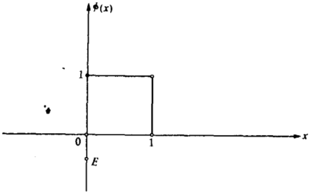


图 3.6.7 方箱函数

supp $\phi(x)$是闭区间时称为紧支撑。方箱函数具有紧支撑。

函数

$$\psi(x)=\begin{cases}1 & x\in\left[0,\ \frac{1}{2}\right)\\ -1 & x\in\left[\frac{1}{2},\ 1\right)\\ 0 & x\in(-\infty,\ 0)\cup[1,\ \infty)\end{cases}$$

称为哈尔函数。它是由方箱函数运算获得的,事实上

$$\psi(x)=\phi(2x)-\phi(2x-1)。$$

哈尔函数的图象如 3.6.8。

哈尔函数是一个母小波函数。如果令

$$\psi_{jk}(x)=\sqrt{2^j}\psi(2^jx-k) \qquad ⑭$$

那么 $\{\psi_{jk}(x),\ j,\ k\in\mathbf{Z}\}$ 是一组正交小波基,其中 Z 表示全体整数的集合。容易证明它是一个正交函数系。

命题 1 $\{\psi_{jk}(x),\ j,\ k\in\mathbf{Z}\}$ 是一个正交函数系。

证明 因为 $0\leqslant 2^jx-k\leqslant\frac{1}{2}$ 等价于

$$\frac{2k}{2^{j+1}}\leqslant x\leqslant\frac{2k+1}{2^{j+1}} \qquad ⑮$$

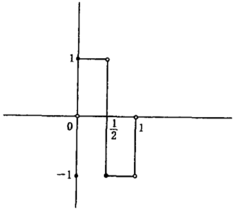


图 3.6.8 哈尔函数

$\frac{1}{2} \leqslant 2^j x - k \leqslant 1$ 等价于

$$\frac{2k+1}{2^{j+1}} \leqslant x \leqslant \frac{2k+2}{2^{j+1}}。 \tag{16}$$

根据哈尔小波基的定义和可得

$$\psi_{jk}(x) = \begin{cases} \sqrt{2^j} & \frac{2k}{2^{j+1}} \leqslant x < \frac{2k+1}{2^{j+1}} \\ -\sqrt{2^j} & \frac{2k+1}{2^{j+1}} \leqslant x < \frac{2k+2}{2^{j+1}} \\ 0 & \text{else} \end{cases}$$

显然有

$$\int_{-\infty}^{\infty} (\psi_{jk}(x))^2 \mathrm{d}x = \int_{\frac{2k}{2^{j+1}}}^{\frac{2k+2}{2^{j+1}}} 2^j \mathrm{d}x = 1 \tag{17}$$

因为 $\psi_{jk}(x)$和 $\psi_{j'k'}(x)$当 $j \neq j'$ 或 $k \neq k'$ 只有两种情况：

1) $\operatorname{supp} \psi_{jk}(x) \cap \operatorname{supp} \psi_{j'k'}(x) = \varnothing$（或仅含区间边界上的个别点），此时乘积为零；

2) $\operatorname{supp} \psi_{jk}(x)$和 $\operatorname{supp} \psi_{jk}(x)$相交成一区间，则易知它必包含其中一个函数的整个非零区间，而另一个函数在该区间上取定值，从而

函数乘积的积分为零。

综合上述两种情况均有

$$\int_{-\infty}^{\infty} \psi_{jk}(x)\psi_{j'k'}(x)\mathrm{d}x = 0 \tag{18}$$

即 $\psi_{jk}(x)$和 $\psi_{j'k'}(x)$正交。

命题 2 定义域为紧集的连续函数总可以展开为小波级数。

这里不加证明。定理说明任一个紧集上的连续函数 $f(x)$总可以表示为:

$$f(x) = \sum_{j=-\infty}^{\infty} \sum_{k=-\infty}^{\infty} C_{jk}\psi_{jk}(x) \tag{19}$$

其中 C_{jk}是小波级数的展开项系数,

$$C_{jk} = \int_{-\infty}^{\infty} f(x)\ \overline{\psi_{jk}(x)}\mathrm{d}x \tag{20}$$

这里 $\psi_{jk}(x)$是小波基,函数上面的一横表示该函数的共轭。

除了哈尔小波基,还有许多其他小波基,例如 Shanon 小波基,墨西哥草帽小波基,Meyer 小波基,Morlet 小波基和 Daubechies 小波基等等。

用如下的 Matlab 函数可以画出不同的小波母函数,然后用⑥得出相应的小波基。

例如,lb =-5; ub = 5; n = 100;(定义图中支撑的长度和在支撑长度中均匀分布着的点的个数)

[psi, x] = mexihat (lb, ub, n);(得到的墨西哥小波函数的值记作 psi)

subplot(221), plot(x, psi); xlabel(图 3.6.9 中"墨西哥草帽小波")

lowb =-8; uppb = 8; n = 1024;

[phi, psi, x] = meyer(lowb, uppb, n);

subplot(222), plot(x, psi); xlabel(图 3.6.10 的"梅耶小波")

subplot(223), plot(x, phi); xlabel(图 3.6.11 的"Meyer 尺度函

数")

lob =－4; upb = 4; n = 1000;

morlet(lob, upb, n); subplot(224), plot(x, psi); xlabel; (图3.6.12的"Morlet小波")

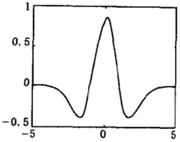


图 3.6.9 墨西哥草帽小波

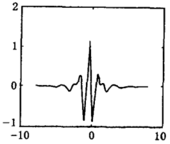


图 3.6.10 梅耶小波

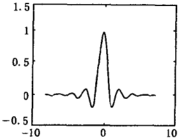


图 3.6.11 Meyer 尺度函数

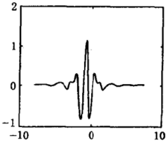


图 3.6.12 Morlet 小波

6. 多尺度分析

方箱函数在小波分析中称为尺度函数。由方箱函数 $\phi(x)$ 可以产生一系列的函数：

$$\phi_{0k}(x) = \phi(x-k),\ k \in \mathbf{Z}$$

$$\phi_{1k}(x) = \phi(2x-k),\ k \in \mathbf{Z}$$

$$\cdots$$

$$\phi_{jk}(x) = \phi(2^j x-k),\ k \in \mathbf{Z}$$

$$\cdots$$

可以证明对于任意 $j \in \mathbf{Z}$, $\{\phi_{jk}(x),\ k \in \mathbf{Z}\}$ 是一组正交的基函

数。令

$$V_j = \{\phi_{jk}(x) \text{ 的线性组合}, k \in \mathbf{Z}\}$$

闭区间上的连续函数 $f(x)$在 V_j 上的(近似)展开是

$$f(x) = \sum_k \langle f(x), \phi_{jk}(x) \rangle \cdot \phi j_{jk}(x)$$

可以证明

$$V_{j+1} = V_j \oplus W_j \quad ㉑$$

其中 $W_j = \{\psi_{jk}(x) \text{ 的线性组合}, k \in \mathbf{Z}\}$，⑮表示 $f(x)$在 V_{j+1} 上的展开等于它在 V_j 上的展开和它在 W_j 上展开之和。

由于

$$V_{j+1} = V_{j-1} \oplus W_{j-1} \oplus W_j, V_{j+1}, V_j, V_{j-1}$$

相当于不同的尺度,因此这种分析称为多尺度分析。

多尺度分析是小波分析的重要内容,它在信号处理中十分有用。

第七节　分形几何概观

分形是 20 世纪初出现的一种研究对象，当时是数学象牙塔中少数奇才发现的“数学怪物”，是不入数学研究主流的“病态”的图形，甚至可以说是一种不登大雅之堂的雕虫小技。

但是到了 20 世纪末，情况出现了根本性的转变。今天，分形已成为一门严肃的数学分支，成为严肃数学家的研究对象；成为一门艺术，一门有着广泛应用的艺术；成为一种工具，图象压缩、信息传输的工具；成为一种上帝创造的指纹，鉴定特定的地质纪元、矿脉类型及其含量的“指纹”。

1. 分形是一种几何

我们熟知的几何是欧几里得几何，有较高数学修养的还知道黎曼几何，非欧几何等等。在这些几何空间中可以引进坐标架，建立坐标，也可以引进维数的概念。一个物体的欧氏维数是能容下它的空间之最低维数，而其拓扑维数则是其独立坐标的个数。

欧几里得几何、黎曼几何、非欧几何等研究的对象是直线、圆、平面、球、锥面等等，这些都是从客观世界中抽象出来的几何对象。因此也可以说欧几里得几何、黎曼几何、非欧几何等是理想化了的几何。

而我们日常生活中见到的山像锥又不是锥，云、树像球又不是球，海岸线、河岸线像折线又不是折线。它们都是具有某种奇异性的几何对象，我们将会看到它们都具有某种分形结构。研究物体的分形结构的几何学称为分形几何。所以，在某种意义上可以说分形几

何是更接近现实的几何。当欧几里得几何、黎曼几何在宏观世界大行其道,罗巴切夫斯基几何在宇宙世界得到应用之时,分形几何理当在微观世界大有用武之地。

2. 分 形 的 例 子

(1) Cantor 集

在许多数学书中提及的 Cantor 集,就是一个一维分形。它的构造过程为:将区间[0, 1]等分为三,去掉中间的一段,将左右两段再一分为三去掉中间一小段,如此重复,余下部分的极限即为 Cantor 集,如图 3.7.1 所示。

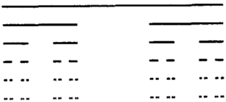


图 3.7.1 Cantor 集的构造过程

(2) 科和雪花

将一条线段分为三段,以中间一段为一边向外作一等边三角形,然后将这一段去掉,加上等边三角形的余下两边,对所得长度为原来 1/3 的四条小线段重复上述操作,即得科和雪花,如图 3.7.2 所示。

(3) Sierpinski 地毯和 Sierpinski 海绵

将一个正方形等分成 9 个小正方形,去掉中间一个,对其余 8 个重复上述过程,即得 Sierpinski 地毯,如图 3.7.3 所示。

将一个正方体等分成 27 个小正方体,将不在大正方体棱边上的 7 个去掉,对余下 20 个重复上述过程,即得 Sierpinski 海绵,如图 3.7.4所示。

(4) 叶子

它是用一组双曲迭代函数对一点进行随机迭代得到的,如图 3.7.5所示。

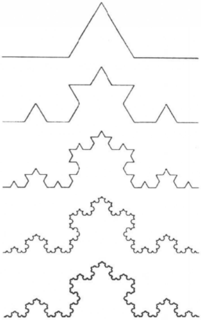


图 3.7.2　科和雪花曲线的构造过程

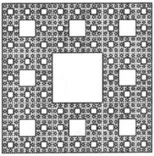


图 3.7.3　Sierpinski 地毯

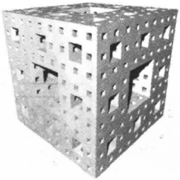


图 3.7.4　Sierpinski 海绵



图 3.7.5　用随机迭代法得到的叶状图形

(5) Mandelbrot 集与 Julia 集

被誉为现代分形之父的 B. B. Mandelbrot(耶鲁大学教授,IBM 公司 T. J. W 研究中心高级研究员,美国国家科学院院士,美国艺术与科学研究院院士)对分形下过如下的定义:

一个集合,如果其 Hausdorff 维数(一种分维)严格大于其拓扑维,则称该集合为分形集。

下面我们来考察几种由极其简单的迭代法则生成的具有意想不到的复杂结构的分形图。考虑复函数(复映射):

$$f(z,\ c,\ p) = z^p + c$$

我们将所有迭代式序列有界的点集之边界集

$$\mathbf{J}(\mathbf{p},\ \mathbf{c}) = \partial\{z:\ z,\ f(z),\ f_2(z),\ \cdots,\ f_n(z),\cdots \text{有界}\}$$

称为裘立雅(Julia,1920)集,而将使得裘立雅集 $\mathbf{J}(\mathbf{p},\ \mathbf{c})$ 连通的所有复数 c 的集合称为曼特勃洛托(Mandelbrot,1980)集。

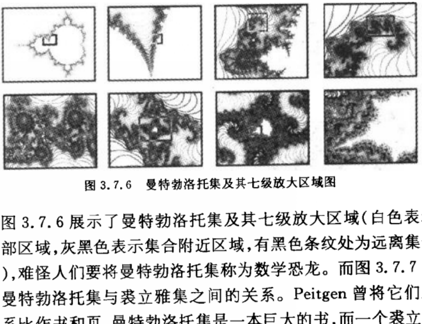


图 3.7.6 曼特勃洛托集及其七级放大区域图

图 3.7.6 展示了曼特勃洛托集及其七级放大区域(白色表示集合内部区域,灰黑色表示集合附近区域,有黑色条纹处为远离集合的区域),难怪人们要将曼特勃洛托集称为数学恐龙。而图 3.7.7 则展示了曼特勃洛托集与裘立雅集之间的关系。Peitgen 曾将它们之间的关系比作书和页,曼特勃洛托集是一本巨大的书,而一个裘立雅集只是其中的一页。根据点 c 在曼特勃洛托集中的位置就能够预测相应的裘立雅集的外形及大小。曼特勃洛托集是一本可以查阅所有裘

立雅集的词典。裘立雅集有自相似性质，而曼特勃洛托集没有这种性质。

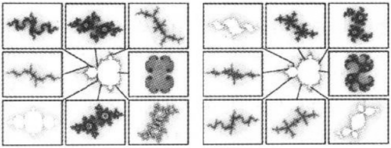


图 3.7.7　曼特勃洛托集与裘立雅集

3. 分形的维数

让我们先来看看几何对象的维数是如何定义的。

维数与测量有密切关系，测量一个几何图形时要用一个与图形的维数 d 相一致的"单位" $l^n(n=d)$ 去测，才会有确定的结果。例如，量体积要用立方体 l^3 为单位，量面积要用正方形 l^2 为单位，量长度要用线段 l 为单位，等等。如果"单位"的维数 n 与几何图形的维数 d 不相等的话，那么 $n<d$ 时结果为无穷大；$n>d$ 时结果为零。也就是说，当 $n \neq d$ 时，这个"单位"不能用来测量几何图形。

事实上，几何与尺度是密切相关的。首先让我们来观察长度和维数与尺度的关系。

如果让两个小组来度量长江的长度，其中一组以 10 米为单位，而另一组以 1 厘米为单位。最后我们发现，两个小组量得的长度有很大的差别，后一组所量得的长度要比前一组量得的大得多。这是因为河岸线、海岸线都具有分形结构，当度量单位趋于零时其长度趋于无穷大。

让我们再来考察一个毛线球的维数。我们先在 200 米的距离上来观看它，这时它是一个点，是零维的。其次在 20 米的距离上来观看它，这时它是一个球，是 3 维的。再在 2 米的距离上来观看它，这

时它是由毛线绕成的一个球，是 1 维的。最后在 2 厘米的距离上来观看它，这时可发现绕成球的毛线是由千丝万缕的绒毛按相似的结构织成的。

分形维数的定义有很多种，如：Hausdorff 维数、自相似维、容量维、信息维、关联维、Lyapunov 维、盒子维等等。下面我们给出自相似维和盒子维的定义。

定义 1 若 $A \in \mathbf{R}^n$ 总可以逐级分成 N 个同样大小的与原集合相似的子集，每次的缩小因子为 $\frac{1}{b}$，则称

$$Ds = \frac{\ln N}{\ln b}$$

为 A 的自相似维数。

例如，Koch 曲线的自相似维数为 $Ds = \frac{\ln 4}{\ln 3} = 1.2619$，Sierpinski 三角形的自相似维数为 $Ds = \frac{\ln 3}{\ln 2} = 1.585$。

定义 2 设 $A \subset \mathbf{R}^n$，用边长为 $\frac{1}{2^n}$ 的小盒子去覆盖 A，$N_n(A)$ 表示盖满 A 所需的最少盒子数，则称

$$D = \lim_{n \to \infty} \frac{\ln N_n(A)}{\ln 2^n}$$

为 A 的盒子维。

盒子维是目前应用最广泛的一种维数，这主要是因为它非常容易由计算机求得。若将边长为 $\frac{1}{2^n}$ 的小盒子改为半径为 ϵ 的小球，则得到容量维。

4. 分形的应用

分形理论已经得到了广泛的应用，例如在装饰设计、图象压缩、

地质和采矿勘探等领域的应用已产生了巨大的经济效益。下面我们介绍吸引子定理在图形模拟及构造分形中的应用。其原理是构建一组适当的线性迭代映射的和

$$f_i(x) = A_i x + E_i,\ i = 1,\ 2 \cdots n$$

利用计算机快速迭代出各种图形,如蒙娜丽莎的像。

设$(X,\ d)$为距离空间,$0 < s < 1$,若映射 $w: X \to X$ 满足

$$d(w(x) - w(y)) \leqslant sd(x,\ y),\ x,\ y \in X,$$

则称 w 为压缩映射。

显见平面上的一个线性变换

$$w(x) = Ax + E,\ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ E = \begin{pmatrix} e \\ f \end{pmatrix}$$

至多有 6 个参数,从而 3 个初始点及其象点可唯一地确定一个线性变换。

若 $w_i(x) = A_i x + E_i$ 为线性压缩映射,则称

$$\{X;\ w_i,\ i = 1,\ \cdots,\ N\}$$

为双曲迭代函数系。

在平面上的一个双曲迭代函数系至多有 $6N$ 个参数。

吸引子定理 若 $\{X;\ w_i,\ i = 1,\ \cdots,\ N\}$ 为一组双曲迭代函数系,则集合映射

$$W(B) = w_1(B) \cup w_2(B) \cup \cdots \cup w_N(B),\ B \subset X$$

也是压缩映射,从而存在唯一不动点 $D \subset X$(即 $W(D) = D$),且对任意 $B \subset X$,

$$W^n(B) = W(W^{n-1})(B) \to D,\ n \to \infty$$

称不动点 D 为双曲迭代函数系的吸引子。

这里,集合间的距离为 Hausdorff 距离 h:

$$d(x,\ B) = \min\{d(x,\ y):\ y \in B\}$$

$$d(A, B) = \max\{d(x, B): x \in A\}$$

$$h(A, B) = \max\{d(A, B): d(B, A)\}$$

现在介绍用确定法在平面 $\mathbf{R}^2$ 上生成吸引子的步骤和例子：

1) 任取平面上一个集合 A_0，

2) 计算 $w_i(A_0)$和 $A_1 = \bigcup w_i(A_0)$，

3) 擦去 A_0 并打上 A_1，

4) 计算 $w_i(A_1)$和 $A_2 = \bigcup w_i(A_1)$，

5) 重复(c)和(d)共 m 次，m 足够大。

例 Sierpinski 三角形的生成过程。

若取定双曲迭代函数系为：

$$w_1: w_{11}(x, y) = \frac{x}{2},\ w_{12}(x, y) = \frac{y}{2}$$

$$w_2: w_{21}(x, y) = \frac{x}{2} + 5,\ w_{22}(x, y) = \frac{y}{2}$$

$$w_3: w_{31}(x, y) = \frac{x}{2},\ w_{32}(x, y) = \frac{y}{2} + 5$$

则显示每个 w_i 将一个正方形变为一个面积为原来$\frac{1}{4}$的小正方形。再取初始集合为 $\{(x, y): 0 \leqslant x \leqslant 10, -10 \leqslant y \leqslant 0\}$（也可任取），即可得到如图 3.7.8 所示的 Sierpinski 三角形。

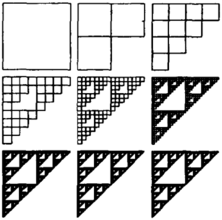


图 3.7.8 用确定法生成 Sierpinski 三角形的过程

除确定法外，生成分形图象的其他方法还有随机迭代法，膨胀法等。

下面考虑反问题：已知分形或某图形（总可将其视为一个分形），求双曲迭代函数系。这时我们可以应用拼贴定理，即利用公式

$$D = W(D) = w_1(D) \cup w_2(D) \cup \cdots \cup w_N(D)$$

形象地说，如果试图找一个 IFS（迭代函数系），使其吸引子与某给定的集合相似或相近，我们必须找一组压缩仿射变换，使得将给定集合分别被各个压缩映射变换后的象（为其自身的各个小"拷贝"）能够拼贴成一个集合，并且该集合在 Hausdorff 距离下尽量地相近于原来给定的集合。

对于一幅很复杂的图像，如果找到了一个可近似该图形的 IFS，其中含有 N 个线性变换，则只需确定 $3N$ 个点及其象，或至多 $6N$ 个参数即可确定或传输这幅图像。这无疑会大大降低数据量。

由上例中双曲迭代函数 w_i 的几何意义，知上面 Sierpinski 三角形的生成过程及后面的习题 2 和 3 可作为已知分形或某图形求双曲迭代函数系的例子。

5. 分形进入中学数学课堂

分形不仅可以进入大学生的数学实验课，还完全可以进入中学数学课堂。它有助于学生更好地认识世界的复杂性，多样性，自相似性，对称性，并在进一步体验到世界之美妙的同时，更好地理解数学、喜爱数学，提高数学的应用能力，增强创造能力和想象能力。

例如中学生熟悉的方程 $x^2 - x - 0.5 = 0$ 的两个实根 $x = \frac{1 \pm \sqrt{3}}{2}$ 可视为迭代映射

$$x_{new} = x_{old}{}^2 - 0.5$$

的两个不动点，其中 $\frac{1+\sqrt{3}}{2}$ 是不稳定的，而 $\frac{1-\sqrt{3}}{2}$ 和无穷远是吸

引子。

将此迭代映射推广到复平面上：

$$z_{new} = z_{old}{}^2 + c$$

即 $$(x+\mathrm{i}y)_{new} = (x+\mathrm{i}y)_{old}{}^2 + (x_c + \mathrm{i}y_c)$$

当取 $x_c + \mathrm{i}y_c = -0.1 + 0.6\mathrm{i}$ 时，初始点 $x_0 + \mathrm{i}y_0 = 0.4 + 0.7\mathrm{i}$ 的轨道(迭代点列)是发散趋于无穷的；初始点 $x_0 + \mathrm{i}y_0 = 0.2 + 0.3\mathrm{i}$ 的迭代点列是收敛的。事实上，

$$x_1 + \mathrm{i}y_1 = -0.15 + 0.72\mathrm{i}$$

$$x_{10} + \mathrm{i}y_{10} = -0.124\,0 + 0.540\,6\mathrm{i}$$

$$x_{98} + \mathrm{i}y_{98} = -0.221\,8 + 0.415\,3\mathrm{i}$$

$$x_{99} + \mathrm{i}y_{99} = -0.223\,3 + 0.415\,7\mathrm{i}$$

根据以上迭代公式编程并进行迭代、绘图，对不同的 c 值即可得到各种不同的吸引域和裘立雅集，详见参考文献[5]。

结　　语

“病态”的几何结构原本是极其自然的，自然界的许多东西的几何图形可以由极其简单的演化规则演化而成。分形理论有助于解释为什么少量的遗传物质(遗传密码)可以发育成极其复杂的结构，正如一条 Peano 曲线可以“填满”一个正方形，占人体 5%的血管布满了人体的每一部分一样。作为一门有着广泛应用的数学分支，分形已经进入各门科学，进入学生的课堂，进入寻常百姓的日常生活，甚至已被制成引人入胜、启迪智慧、老少皆宜、百看不厌的“连环画”。

练习

1. 计算 Sierpinski 垫片的分维数。

2. 已知 Sierpinski 三角形位于区域 $\{x\geqslant 0,\ y\geqslant 0,\ x+y\leqslant 20\}$

之中，试求生成此分形的迭代函数系。

提示：$N=3$，先在两个方向上各压缩至$\frac{1}{2}$，再将原点分别平移至(0, 0)，(0, 10)和(10, 0)，初始正方形为$[1, 20]\times[1, 20]$。

3. 试求生成Koch曲线的迭代函数系（位于矩形$[0, 3]\times[0, 1]$内）。

提示：$N=4$，先在两个方向上各压缩至1/3，然后对w_1，w_2将原点分别平移至(0, 0)和(2, 0)；对w_3先旋转$\pi/3$，再平移(1, 0)；w_4先平移(−1, 0)，再旋转$-\pi/3$，再平移(2, 0)。

w_3，w_4也可用三点确定一个线性映射来给出。w_3分别映(0, 0)，(0, 3)和(3, 0)为(1, 0)，$(1-\sqrt{3}/2, 1/2)$和$(3/2, \sqrt{3}/2)$，w_4分别映(0, 0)，(0, 3)和(3, 3)为$(3/2, \sqrt{3}/2)$，(2, 0)和$(2+\sqrt{2}/2, 1/2)$。

参考文献

[1] 奇妙的分形. 吴宝丰、袁震东. 数学教学，2000年第3期，28—30.
[2] 潘金贵、艾早阳. 分形艺术程序设计. 南京大学出版社，1998.
[3] 王东生、曹磊. 混沌、分形及其应用. 中国科学技术大学出版社，1995.
[4] 高安秀树. 分数维. 沈步明、常子文译. 地震出版社，1994.
[5] Math in School, 23:3(1994), 3—7.

第八节　混沌现象:非线性数学

在我们生活的这个真实的世界中,混沌现象无时不有,无处不在。为什么天气变化存在着不可预测性？为什么气体和流体会从平稳流动突然变为紊流？为什么两个形式和意义极不相同的迭代方程的相邻倍周期参数值的比率收敛于同一个 Feigenbaum 常数？这就是混沌在起作用。人们预感到,这些深奥问题的解决很可能揭示大自然更深一层的规律。

正是对这些问题的研究,诞生了一门新的科学——混沌学。混沌学目前在各个领域都得到广泛的应用,正如混沌学倡导者之一的 M. Shlesinger 所说:“20 世纪科学将永远铭记的只有三件事,那就是相对论、量子力学和混沌。”

早在公元前 560 年左右,我国古代思想家老子就提出了宇宙起源于混沌的哲学思想。而公元前 450 年左右,古代哲学家庄子则把混沌的思想引入政治学的研究中。他说:“南海之帝为倏〔su,倏地,极快地〕,北海之帝为忽〔灵敏〕。中央之帝为混沌。”

1903 年,动力系统的创始人 Poincare 首先在他的研究工作中指出了混沌存在的可能性。1954 年,前苏联概率论大师 A. N. Kolmogorov 的工作也为混沌思想的萌芽作出了突出的贡献。但真正的混沌研究开始于 20 世纪 60 年代。Lorenz 用一台原始计算机研究气候的变化,发现了气候不能精确重演,小的变化可以放大为大的变化,即对初始条件的极端敏感性,如著名的蝴蝶效应:巴西一只蝴蝶翅膀的振动会引起纽约的一场大雨。

20 世纪 70 年代是混沌发展史上成果辉煌的年代。李天岩、J. Yoke 在 1975 年证明了“周期 3 隐含着混沌”;1975 年生物学家 R.

May 在《自然》杂志上发表文章证明了简单确定的数学模型可以产生类似于随机的混沌行为，但混沌中又有惊人的有序性。1978 年，M. J. Feigenbaum 揭示了一类一维非线性映射在通过倍周期分叉演变到混沌的过程中有两个所谓的普适常数——Feigenbaum 常数。一方面是普适的铁定的规律；一方面是混沌，它们相辅相成。与此同时，经济学家们在尝试用混沌的思想和方法来研究股票价格变动的大致规律。

20 世纪 80 年代混沌学进一步发展。有关混沌研究的学术会议一场接一场，相应的学术研究刊物接二连三地创刊。1980 年，数学家 Mandelbrot 在 IBM 研究中心的计算机上绘出了第一张精美绝伦、复杂无比、被称为"数学恐龙"的 Mandelbrot 集的图像。从此这种图像便成为混沌的标志。1986 年，徐京华院士提出神经网络中存在混沌，人脑是一个复杂的多层次的混沌动力系统。混沌不是病态，混沌萌生信息。正常人的脑思维是混沌的，而白痴的脑活动几乎没有混沌。

20 世纪 90 年代，混沌科学向其他科学进一步渗透，混沌在生物、生理、心理、物理、化学、电子、信息、天文、气象、经济、音乐、艺术等领域都得到了广泛的应用。

1. 二次函数产生的混沌

让我们从昆虫的繁殖说起。夏日的蝉是每年都会看见的，但品种繁多。有一种十七年蝉，成虫只活几星期，然后产下大量卵，孵化成幼虫后钻入地下，附在树根上 17 年，然后再羽化成蝉。因此这种蝉每 17 年大量出现一次，此外还有 13 年蝉、7 年蝉、4 年蝉等。

描写昆虫种群的变化，可以通过迭代方程 $x_{n+1} = f(x_n)$ 来描述。数学上最常处理的是下述迭代关系（由二次函数 $\lambda x(1-x)$ 作成）：

$$x_{n+1} = \lambda x_n(1 - x_n),\ 0 \leqslant \lambda \leqslant 4,\ n = 1, 2, \cdots$$

我们设 x_n 是某昆虫种群第 n 代的虫口数，$f(x)$ 是它的繁殖曲

线，那么将有

$$x_n = f(x_{n-1}) = f(f(x_{n-2})) = \cdots = \underbrace{f(f\cdots f}_{n}(x_0)\cdots)$$

以后记 f^n 为 f 的 n 次复合。称 x_0 是 $f^n(x)$的不动点，若

$$f^n(x_0) = x_0$$

我们也称 x_0 是 $f(x)$的 n 周期点。下面分析迭代情形。

1) $0 < \lambda < 1$, $f(x) = \lambda x(1-x)$ 有两个不动点，因为

$$x = \lambda x(1-x)$$

的解是

$$x^* = 0 \text{ 和 } x^* = 1 - \frac{1}{\lambda}$$

此时 $x^* < 0$ 不合题意，故只有 $x^* = 0$ 是不动点。从图形上看，不动点 x_0 就是 $f(x)$和 $y = x$ 的交点处的横坐标。任何初值 x_0 经过迭代后都会收敛于不动点 0（见图3.8.1）。

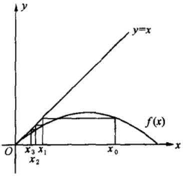


图 3.8.1

2) $1 < \lambda < 3$，此时 $f(x) = \lambda x(1-x)$ 仍有两个不动点

$$x = 0,\ x = 1 - \frac{1}{\lambda}$$

任取初始值 x_0，迭代后一定收敛于 $1-\frac{1}{\lambda}$。0 虽然也是不动点，但是任何不为零的初始值 x_0，无论如何接近于零，却不会收敛于 0 点，而会收敛于 $1-\frac{1}{\lambda}$。这时 0 是排斥子，$1-\frac{1}{\lambda}$ 是吸引子（见图 3.8.2）。

3) $3 < \lambda < 1+\sqrt{6} \approx 3.449$，这时的不动点仍为

$$0 \text{ 和 } 1-\frac{1}{\lambda}$$

但它们都是排斥子。我们从图 3.8.3 中可看出，由初值 x_0 出发得出 x_n 不收敛于 0，也不收敛于 $1-\frac{1}{\lambda}$，而是在两个点的附近来回变动（见图3.8.3）。

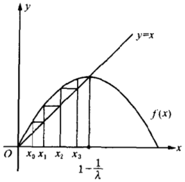


图 3.8.2

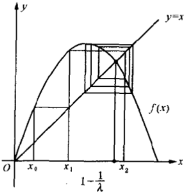


图 3.8.3

经计算，这两个点是

$$f^2(x)=f(f(x))=\lambda^2 x(1-x)[1-\lambda x(1-x)]$$

的不动点，它有 4 个解：

$$0,\ 1-\frac{1}{\lambda},\text{和}\frac{1}{2\lambda}(1+\lambda\pm\sqrt{(\lambda+1)(\lambda+3)})$$

这说明当 $\lambda>3$ 后，不动点 $1-\frac{1}{\lambda}$ 由吸引子转为排斥子，同时派生出两个吸引的 2 周期点：

$$x_{11}=\frac{1}{2\lambda}(1+\lambda+\sqrt{(\lambda+1)(\lambda+3)})$$

$$x_{12}=\frac{1}{2\lambda}(1+\lambda-\sqrt{(\lambda+1)(\lambda+3)})$$

$$f(x_{11})=x_{12},\ f(x_{12})=x_{11}$$

$$f(f(x_{11})) = x_{11},\ f(f(x_{11})) = x_{12}$$

④ $1+\sqrt{6}<\lambda<3.544$，这时两个 2 周期点又将分化为四个 4 周期点：

$$\begin{array}{ccc} 0.3828 & \longrightarrow & 0.8269 \\ \uparrow & & \downarrow \\ 0.8750 & \longleftarrow & 0.5009 \end{array}$$

随着 λ 的增大，f 的周期点个数不断增加。这种一分为二，二分为四的过程，称为分歧过程。参数 3 是一分为二的分歧值，$1+\sqrt{6}$ 是二分为四的分歧值。可以算出，$\lambda = 3.544,\ 3.564$ 时分别是四分为八，八分为十六的分歧值。这一分歧过程会不断发生，分歧值越来越靠近，收敛于 $\lambda = 3.569\,945\,972$ 时，出现周期为∞的解，此时即进入混沌状态，任何初值的迭代都不会收敛于有限的值（吸引子），x_n 将在整个[0, 1]上游荡，好像可以随机地出现在任何位置上，完全没有规律可循。

这自然是一个深刻的发现。从确定的现象（一个二次函数 $\lambda x(1-x)$）通过迭代居然能产生出随机性现象，这就把两种完全不同类型的数学问题沟通起来了。这个深刻的发现，使人不禁感叹大自然规律的神奇。

事情尚未到此完结，70 年代末期，美国康奈尔大学的菲根鲍姆(Feigenbaum)从上述的迭代过程中发现了普适常数 4.669 201 629 …，见下表：

周期倍化分歧中间距比值变化情况

m	分歧情况	分歧值	间距比值 $\frac{\lambda_m - \lambda_{m-1}}{\lambda_{m+1} - \lambda_m}$
1	1 分为 2	3	
2	2 分为 4	3.449 489 743	4.751 466
3	4 分为 8	3.544 090 359	4.656 251
4	8 分为 16	3.564 407 266	4.668 242

（续表）

m	分歧情况	分歧值	间距比值 $\frac{\lambda_m - \lambda_{m-1}}{\lambda_{m+1} - \lambda_m}$
5	16 分为 32	3.568 759 420	4.668 74
6	32 分为 64	3.569 691 610	4.669 1
⋮	⋮	⋮	⋮
∞	混沌	3.569 945 972	4.669 201 629

菲根鲍姆对许多迭代函数进行了大量的计算，都得到 4.669 201 629…这个数，这决非巧合。尽管目前还不清楚这个数的本质，但学术界倾向于认为它是自然界中的普适常数，此即著名的菲根鲍姆常数。

现在世界上至少有几千名学者热衷于混沌理论，期望这一现象的研究会揭示宇宙的奥秘。

2. 周期 3 则乱七八糟

让我们回到数学上来。1974 年 4 月的一天，美国马里兰大学的博士研究生李天岩走进他的导师——约克(J. A. Yorke)教授的办公室，约克随口对李天岩说："试试区间迭代怎么样？"一个星期以后，李天岩证明了如下结果：

定理 若 $f(x)$是区间$[a, b]$上的连续自映射，且有一个 3 周期点，则对任何正整数 $n > 3$，都有 n 周期点。

这一定理看上去很简单，李天岩和约克联名向《美国数学月刊》投稿。这是一本中级数学杂志，在 1975 年出版的第 82 卷第 985 页至 992 页上李天岩和约克的文章登了出来。题目是"Period Three Implies Chaos"，按李天岩本人的译法就是"周期 3 则乱七八糟"。这篇不起眼的小文章，由于通俗易懂，读者很多，物理学家也接受了。随之而来的便是 Chaos 热(Chaos 中译为混沌)。现在，它已发展为研究混乱现象(湍流、分形)的基础理论了。

这个定理的结论虽然很简单，但是并不直观。试看下图中的函数，它虽然有一个 3 周期点 0：

$$f(0)=\frac{1}{2},\ f\left(\frac{1}{2}\right)=1,\ f(1)=0$$

但你能看得出来，它会有 4 周期点、5 周期点，以至对任意 n 的 n 周期点？显然这不是靠直观能办到的事，必须用数学的方法严格证明。（这个定理的证明并不难，主要用初等方法。有兴趣的读者可参看 1985 年的《自然杂志》上刊登的“从平凡的事实到惊人的定理”）

3. 混沌的定义

（1）李—约克的定义

记 I 为区间，映射 $f: I\rightarrow R$ 连续，$f^2(x)=f(f(x))$，$f^n(x)=f(f^{n-1}(x))$，称

$$Orb_f(x)=\{\cdots, f^{-n}(x), \cdots, f^{-1}(x), x, f(x), \cdots, f^n(x), \cdots\}$$

为 f 过 x 的轨道。

若 $f(x)=x$，则称 x 为 f 的不动点。若

$$f^n(x)=x,\ f^i(x)\neq x,\ i=1,\cdots,n-1$$

则称 x 为 f 的 n—周期点，称 n 为周期。用 $T(f)$ 表示 f 的全体周期集合，$P(f)$ 为 f 的周期点集合。

定义 1 假设 $T(f)=N$（正整数集），且存在不可数集 $S\subset I$，使得

1）对任意 x、$y\in S$，$x\neq y$，

$$\liminf_{n\rightarrow\infty}|f^n(x)-f^n(y)|=0$$

$$\limsup_{n\rightarrow\infty}|f^n(x)-f^n(y)|>0$$

2）对任意 $x\in S$，$y\in P(f)$，

$$\lim_{n\to\infty}\sup \mid f^n(x) - f^n(y) \mid > 0$$

则称 f 为混沌的。

在此定义下，李—约克证明了 $3 \in T(f)$ 隐含着混沌。后来人们发现，李—约克结果中的一部分是俄罗斯数学家 Sarkovskii 于 1964 年获得的下述定理的推论。

将全体自然数按所谓 Sarkovskii 序从小到大排列如下：

$$\begin{array}{ccccc} 3, & 5, & 7, & \cdots & \\ 3\times 2, & 5\times 2, & 7\times 2, & \cdots & \\ 3\times 2^2, & 5\times 2^2, & 7\times 2^2, & \cdots & \\ \cdots, & & & & \\ \cdots, & 2^3, & 2^2, & 2, & 1 \end{array}$$

Sarkovskii 定理 若 $m < n$, $m \in T(f)$，则 $n \in T(f)$。

尽管如此，李—约克结果的贡献不容低估。关于线段上的连续自映射，特别是 Logistic 映射，迄今已发表近 2 000 篇论文，其中有许多引人入胜的结果，如混沌的存在域、导致混沌的途径——倍周期分叉、鞍结点分叉、Feigenbaum 常数等等。有兴趣的参见文献[1]等。

李—约克的定义不尽完美，且局限于线段映射。下面给出两种更为严谨的定义。

(2) 拓扑传递

定义 2 设 $f: M \to M$ 连续，若存在 $x \in M$ 使得轨道 $Orb_f(x)$ 的闭包等于 M，也即 M 中存在 f 的一条稠密轨道，则称 f 是拓扑传递的。

可证，f 是拓扑传递的当且仅当对任意非空开集 $U, V \subset M$，存在 $N = N(U, V)$，使得 $f^N(U) \cap V \neq \varnothing$。

(3) 拓扑混合

定义 3 f 是拓扑混合的当且仅当对任意非空开集 $U, V \subset M$，存在 $N = N(U, V)$，使当 $n > N$ 时，$f^n(U) \cap V \neq \varnothing$。

理解拓扑混合的最好的例子是揉面团。当面团充分揉合时，原

来任意两处的小面团都充分搀和在一起。若在任意两处分别滴上红、绿两种颜料，经充分揉合后两块颜料变成红、绿细丝看似紊乱其实又很有规则地缠绕在一起。揉合越充分，则缠绕得越混乱。

容易看出，拓扑混合隐含着拓扑传递。在动力系统中，通常把具有拓扑混合性质的动力学性态称为混沌。

4. 符号动力系统和马蹄映射

直接通过验证拓扑混合去判定一个系统是否混沌是很困难的。下面介绍一种研究混沌的最简单、最理想的数学模型——符号动力系统。

记 $S_N = \{1, 2, \cdots, N\}$，赋以离散拓扑(即每个孤立点都既是开集，又是闭集)，S_N 成为拓扑空间。定义双边符号序列空间

$$\Sigma_N = \{a: a = \cdots a_{-n}, \cdots a_{-1}a_0a_1\cdots a_n\cdots, a_i \in S_N, i \in \mathbf{Z}\}$$

对任意 $a \in \Sigma_N$，$s \leqslant r$，称

$$I_{sr}(a) = a_s a_{s+1} \cdots a_r$$

为 a 的 sr 节段，$r-s$ 为其长度。称

$$H_{sr}(a) = \{w: I_{sr}(w) = I_{sr}(a)\}$$

为 a 的相应于节段 $I_{sr}(a)$ 的柱状邻域。而称 $U \subset \Sigma_N$ 为开集，若对任意 $a \in U$ 存在 s，r，$s \leqslant r$，使

$$H_{sr}(a) \subset U$$

在上述定义下，Σ_N 是紧致的 Hausdorff 空间。这里，柱状邻域 $H_{sr}(a)$ 相当于欧氏空间中的球状邻域。$r-s$ 越大，邻域越小。

在 Σ_N 中引进距离

$$d(a, b) = \sum_{-\infty}^{\infty} d(a_n, b_n)/2^{|n|}, \quad a, b \in \Sigma,$$

$$d(a_n, b_n) = \begin{cases} 0 & a_n = b_n \\ 1 & a_n \neq b_n \end{cases}$$

易证 Σ_N 同胚于一个 Cantor 集，即在 Σ_N 与某 Cantor 集之间存在着一个一一对应 h，使得 h 和 h^{-1} 都是连续的。为直观地理解 Σ_N 的 Cantor 集结构，让我们将区间 $I = [0, 1]$ 作 $2N-1$ 等分，取其中不相邻的 N 段；再将其中的每一段作 $2N-1$ 等分，再取其中不相邻的 N 段；……无限重复。最后生成的点集称为 Cantor $2N-1$ 分集，记为 C_N。不难看出存在着同胚 $h: \Sigma_N \to C_N$。

在 Σ_N 上定义移位映射 $\sigma: \Sigma_N \to \Sigma_N$，

$$a \to \sigma(a), \ \sigma(a)_i = a_{i+1}, \ i \in Z$$

即
$$a = \cdots a_{-n}, \ \cdots a_{-1} \ \dot{a}_0 a_1 \cdots a_n \cdots$$

$$\sigma(a) = \cdots a_{-n+1}, \ \cdots a_0 \ \dot{a}_1 a_2 \cdots a_{n+1} \cdots$$

可以证明 $\overline{P}(\sigma) = \Sigma_N$，$\sigma: \Sigma_N \to \Sigma_N$ 是拓扑传递的和拓扑混合的，故 σ 具有极其复杂的动力学行为。

这里，我们构造性地证明 σ 有一条稠密轨道。对 $k = 0, 1, 2, \cdots$ 取 $a \in \Sigma_N$，使 a 的所有长度为 k 的节段取遍 S_N 中所有 $k+1$ 个元素(可重复)的所有不同的排列，则它可遍历 Σ_N 中的任意柱状邻域。

对映射 $f: M \to M$，若能证明其存在不变集 Λ (即 $f(\Lambda) = \Lambda$)，使得 $f|_\Lambda$ 与 σ 是拓扑共轭的，即存在同胚 $h: \Lambda \to \Sigma_N$，使得

$$h \circ f|_\Lambda = \sigma \circ h$$

则称 f 以移位映射为其子系统，或称 f 具有移位不变集 Λ，从而 $f|_\Lambda$ 是混沌的。

由 $h \circ f^n = \sigma^n \circ h$ 知，拓扑共轭的两个系统的轨道一一对应。故以移位映射为其子系统已成为混沌的代名词。

下面介绍一种最简单的以移位映射为其子系统的动力系统——马蹄映射，或称 Smale 马蹄，因而它本身也成了混沌的另一个代名

词。其实，所谓 Smale 马蹄映射就是一种揉面团。下面我们将这种"揉"的过程用数学符号描述出来。

考虑 R^2 上的正方形(相应于一个面团)，

$$I = [-1, 1] \times [-1, 1]。$$

定义光滑映射 $f: I \to R^2$ (如图 3.8.4)：

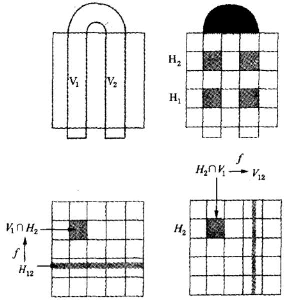


图 3.8.4

先竖向拉长为 λ 倍，横向压缩为 μ 倍，再如图 3.8.4 折叠成马蹄形置于 I 上(相当于将面团揉长揉细，再对折复位)，其中 $\lambda > 2$，$\mu < 1/2$。记

$$f(I) \cap I = V_1 \cup V_2,\ f^{-1}(I) \cap I = H_1 \cup H_2$$

$$H_1 = f^{-1}(V_1),\ H_2 = f^{-1}(V_2)$$

$$H_{ij} = f^{-1}(V_i \cap H_j) = H_i \cap f^{-1}(H_j)$$

$$V_{ji} = f(H_i \cap V_j) = V_i \cap f(V_j)$$

H_i，V_i 的厚度和宽度均小于 1，$H_{ij} \subset H_I$，$V_{ji} \subset V_i$。

归纳地，有

$$
\begin{aligned}
H_{i_0 i_1 \cdots i_k} &= f^{-1}(V_{i_0} \cap H_{i_1 \cdots i_k}) \\
&= H_{i_0} \cap f^{-1}(H_{i_1 \cdots i_k}) \\
&= H_{i_0} \cap f^{-1}(H_{i_1}) \cap f^{-2}(H_{i_2}) \cap \cdots \cap f^{-k}(H_{i_k})
\end{aligned}
$$

$$
\begin{aligned}
V_{i_{-k} \cdots i_{-1} i_0} &= f(H_{i_0} \cap V_{i_{-k} \cdots i_{-1}}) \\
&= V_{i_0} \cap f(V_{i_{-k} \cdots i_{-1}}) \\
&= V_{i_0} \cap f(V_{i_1}) \cap f^2(V_{i_2}) \cap \cdots \cap f^k(V_{i_{-k}})
\end{aligned}
$$

它们分别是厚度 $< 2^{-k}$ 的横条和宽度 $< 2^{-k}$ 的竖条。无穷地做下去，得到 $H_{i_0 i_1 \cdots i_n \cdots} \subset H_{i_0}$ 为一条横线，$V_{\cdots i_{-n} \cdots i_{-1} i_0} \subset V_{i_0}$ 为一条竖线。

$$
\Lambda = \{x:\ x = H_{i_1 \cdots i_n \cdots} \cap V_{\cdots i_{-n} \cdots i_{-1} i_0}\}
$$

为 f 不变集，且存在一一对应

$$
h:\ \Lambda \to \Sigma_2
$$

$$
x = V_{\cdots i_{-n} \cdots i_{-1} i_0} \cap H_{i_1 \cdots i_n \cdots} \to a \in \Sigma_2,\ a_k = i_k
$$

易证 h 是同胚，且 $h \circ f|_{\Lambda} = \sigma \circ h$，这就证得 Smale 马蹄映射 f 存在不变集 Λ，使得 $f|_{\Lambda}$ 拓扑共轭于一个移位映射。换言之，马蹄映射具有移位不变集，所以是混沌的。

当然，上面介绍的以揉面团为原型的马蹄型拓扑映射完全是人为的。为了使其适合于真实的系统，J. Moser(1979)将马蹄映射一般化，并给出了验证一个系统是否具有马蹄的两组条件——Moser 条件。后来，Moser 条件又被推广到高维系统，而符号动力系统的符号集 S_N 也被推广为 S_∞，甚至为一个区间。

习题

(1) 已知同胚 f: $M \to M$ 与 σ: $\Sigma_N \to \Sigma_N$ 是拓扑共轭的，试证 $h \circ f^n = \sigma^n \circ h$，其中 n 为任意整数。

(2) 对映射 σ: $\Sigma_2 \to \Sigma_2$，指出其有几个 1—周期，2—周期，3—周

期轨道。

参考文献

[1] 王东生、曹磊. 混沌、分形及其应用. 中国科学技术大学出版社，1995.
[2] 朱德明、韩茂安. 光滑动力系统. 华东师范大学出版社，1993.
[3] S. Wiggins. Global Bifurcation and Chaos. Springer-Verlag, New York: 1988.

第九节 时间与空间的数学

茫茫太空，遥遥未来，我们生活的宇宙空间究竟是什么样？这是一个永恒的科学主题。古往今来，不知有多少科学志士为此付出毕生精力，但是研究至今仍未完结。一部数学发展史，竟也和这一课题结下了不解之缘。各种各样的几何学正是描摹宇宙的数学框架。请看：

- 按照哲学原理时间是没有起点的。但是人们可以人为地选择一个标志性时间作为计算的原点。此前的时间无限，此后的时间也是无限的。现在世界通行的计算时间的原点是公元零年。尽管这是“耶稣基督”降生的年份，带有明显的宗教色彩。但是，国际上需要一个共同的计算时间的方法。只要大家接受、世界通行，作为“地球村”的一员，就应该遵守国际惯例，和国际接轨。而诸如光绪 XX 年、民国 XX 年的纪年方法确实没有必要再使用了。
- 时间的几何模型是一维的直线。没有开端也没有终结。时间和实数集构成一一对应。时间的连绵不断，正是实数连续性的直观背景。有了年的起点，天文学便要规定月、日、小时、分、秒，以至毫秒、微秒等等，单位越来越小，永远不会完结。一个具体的时刻可以说成是某年某月某日某时某分某秒。用数字来表示，便是一个有理数。另一方面，时间与时间之间是连续的，没有“非时间”的空隙存在。所以时间可以用一条两头无限的直线加以表示。当取定了时间原点和单位时间之后，每个时刻都对应一个实数，每个实数也确定一个时刻。就是说，时间和实数是一一对应的。用几何

方法表示就是一条直线。

- 现实空间的直观描述是三维的:上下、前后、左右。各向同性:无限广延;处处都有一样的密度;每一个维度相当于一条直线;两个维度构成一个平面。古希腊数学家研究点、线、面的关系,更建立起公理体系,世称“欧氏空间”,其上的几何学即“欧氏几何学”。
- 一维几何是贫乏的,平面几何、立体几何就相当复杂。除了直线、直方形,还有曲线,曲面等各种几何形。最简单的曲线是圆,最简单的几何体有柱体、锥体、台体和球体。他们的表面是最简单的曲面,包括柱面、锥面、球面。这种研究方法称为综合几何学的方法。
- 笛卡儿发明了坐标系。把欧氏空间的点变成有序的三元数组(x, y, z);曲线用只有一个参数的方程表示;曲面则用含有两个参数的方程表示;用代数方法进行演算,使得几何学插上了翅膀。用综合方法研究的圆锥曲线,在代数上表示为二次曲线。解析几何学由此诞生。
- 平面和空间的几何学是直观的,但是更高维的几何学需要新的抽象表示方法。平面向量、空间向量推广到 n 维向量,用向量构成了线性空间,矩阵成为描述几何变换的有力的工具。线性代数和几何学成为密切的伙伴。
- 欧氏几何中平行公理的研究,导致非欧几何学的产生。其实,现实世界并非只有一种几何——欧氏几何学。例如球面上的几何学(以大圆作“直线”看)就不满足欧氏平面几何的公理体系。19 世纪发现的非欧几何学打开了新的天地。
- 几何图形可以搬来搬去,不改变图形的面积、体积。中国有所谓“出入相补”原理即基于此种想法。但是相似变换可以把图形放大缩小,面积体积随之而变化。把物体投影在墙上,形状有变化的成分,也有不变的成分。这种变和不变成了几何学的研究对象。射影几何学成了一门学问。F·克莱因提出,几何学应当按变换群进行分类,变换群的不变量

构成几何学的研究对象。

- 欧氏几何学所使用的工具很简单，所以只能研究直线、平面、直方体的变化。由“直”向“曲”的进化，来自微积分的推动。高斯一般地研究曲面上的几何学，即经典的微分几何学。最简单的曲面是球面，地球相当于一个椭球面。地球上两点之间以怎样的曲线为最短？这相当于问，从上海到洛杉矶，沿着怎样的路线走向最短。这种“曲面上的最短线”称为测地线。球面上的测地线就是大圆。
- 微分几何学的一个根本问题是如何“度量”曲线的长短。曲线的弧长当然要用微积分方法进行计算。高斯给出了一系列的基本量度，其中最重要的是曲率。曲面上各处的弯曲程度是不一样的，不像欧氏几何到处都是一样的平直（曲率到处是零）。
- 从平直的欧氏空间进到弯曲的一般空间，不仅仅是弯曲程度起了变化，更重要的是整体结构有改变。我们在前面已经看到过球面、环面具有很不相同的结构。可是人们注意到球面和环面以及许多曲面，从局部看都差不多，环面上一点周围的一小片和球面上一点周围的一小片没有什么大的不同，都可以和欧氏平面上的一个小圆片一一对应起来，好像可以看作和小圆片有一样的结构。曲面之间区别的关键在于整体。比如球面不能和一块小圆片一一对应，必须把球面割成两片，使得每一片和小圆片一一对应。这种把曲面看成许多小块圆片堆积而成（堆成不同的结构）的观点，就是近代几何学家所说的流形。流形的整体结构就是拓扑学的研究对象。
- 20世纪初，爱因斯坦创立“狭义相对论”。他把一维的时间和三维的欧氏空间放在一起考察。引起了物理学的革命。数学上的四维空间成为现实的对象。1910年代爱因斯坦又创立“广义相对论”，把宇宙看成是弯曲的四维空间。这样微分几何学和高维几何学结合起来。宇宙空间原来也是

一种流形。拓扑结构、流形上的距离、高维几何对象的描述方法一下子提出了无数的几何学问题。几何学在 20 世纪下半叶成为数学发展的主流学科。直到今天，几何学仍然是当代数学的生长点。我们对时间和空间的认识还远远没有完结。

下面让我们仔细地在一些关节点上进行剖析。

1. 欧氏空间和坐标几何

“前不见古人，后不见来者，念天地之悠悠，独怆然而涕下。”这是唐朝陈子昂的诗句，抒发着诗人对时间和空间的万千感慨。

就感性认知而言，人只能认知有限的事物，从生到死的时间段，从他目力所及的领域，就是一个人的时间和空间感知范围。但是人还可以想象，用理性来认识世界，就会得到陈子昂那样的印象：时间无始无终，天地无边无沿。

欧几里得的几何学是现实世界最简单、最粗略的近似。他为牛顿的绝对时空准备了数学模型。在牛顿看来，空间像一个大容器，物体在其中运动、静止、放进或移出，空间并不会发生什么变化。另一方面，时间像一条川流不息的河流，无论事件发生或者不发生，时间总是均匀不变地流逝。因此，三维的欧氏几何学可以描述空间，一维的欧氏空间（数轴）可以描述时间，两者互不相干，这是人们最朴素的时空观，也是现今大多数人持有的时空观。在人们日常生活中，用这样的方法描述宇宙也就可以了。

笛卡儿为欧氏空间安上了坐标架，使数形结合起来诞生了解析几何学。用三维的空间解析几何来描述宇宙，增加了“数”的描摹手段，自然有更大的表现力。但是，这也给人们带来了新的问题。这就是，坐标原点如何选择？三根两两垂直的坐标轴的指向如何确定？换句话说，由于宇宙本来没有坐标，坐标原点和坐标轴的架设完全是人为的，各人可以有各人的笛卡儿坐标系。但是空间中物体的形状、位置和运动是客观存在的，不依坐标系的选择不同而有所改变。例

如，线段 AB 的长度，$\triangle ABC$ 的形状在各种坐标系下应该是一样的。所以说，在解析几何学中我们所研究的几何对象乃是那些与坐标系选择无关的量，即在坐标变换下的不变量。

坐标变换是数学家所熟悉的。三维欧氏空间中的两个坐标系 $O\text{—}xyz$ 和 $O_1\text{—}x_1y_1z_1$，如以 $O\text{—}xyz$ 为基准，点 O_1 在坐标系 $O\text{—}xyz$ 中坐标为 (d_1, d_2, d_3)，那么任何点 A 的两种坐标 (x, y, z) 和 (x_1, y_1, z_1) 之间满足关系

$$\begin{cases} x_1 = a_{11}x + a_{12}y + a_{13}z + d_1 \\ y_1 = a_{21}x + a_{22}y + a_{23}z + d_2 \\ z_1 = a_{31}x + a_{32}y + a_{33}z + d_3 \end{cases}$$

其中 (a_{ij}) 是正交矩阵。

如果 Oz 与 O_1z_1 平行，那么坐标变换公式就简化为

$$\begin{cases} x_1 = x\cos\theta + y\sin\theta + d_1 \\ y_1 = -x\sin\theta + y\cos\theta + d_2 \\ z_1 = z + d_3 \end{cases}$$

其中 θ 是 Ox 与 O_1x_1 的夹角。这是平面坐标系的平移与旋转。欧氏几何正是研究在上述变化下的不变性问题。如保持长度与角度不变，保持全等与相似不变，图形面积不变等等。高等代数告诉我们，全体正交变换构成群（欧氏变换群），欧氏几何正是研究这一群下的不变量的几何学。

2. 欧几里得几何与非欧几何

众所周知，欧几里得几何学已经沿用了二千多年，至今中学教材中的几何学内容还是与早在公元前 300 年左右的欧几里得所写的“几何原本”的内容基本一致。然而几何学在 19—20 世纪中经历了十分重大的变化和发展。在“几何原本”中，欧几里得先对一些基本概念（如点、直线、平面等）给出了定义：

点没有大小；

线有长度，但没有宽度；

线的界限是点(注："几何原本"中没有伸展到无穷的线)；

直线是同其中各点看齐的线；

面只有长度和宽度；

面的界限是线；

平面是与其上的直线看齐的那种面；

圆是包含在一条(曲)线里的那种平面图形，使得从其内部某一点连到该线的所有直线(线段)都彼此相等，并称圆内上述的那个点为圆的中心(简称圆心)；

平行直线是在同一平面内，而且往两个方向无限延长后，在这两个方向上都不会相交的直线。

欧几里得总共引入了 119 个定义，承认了五条公设：

等于同量的量是相等的；

等量加等量还是等量；

等量减等量还是等量；

能重合的量是全等的；

整体大于部分。

接着，欧几里得再给出了五个公理：

1) 从每个点到每个其他的点必定可以引直线。

2) 每条直线都可以无限延长。

3) 以任意点作中心，通过任何给定的另一点，可以作一圆。

4) 所有直角都相等。

5) 同平面内如有一条直线与另两条直线相交，且在前一条直线的某一侧所交的两内角之和小于两直角，则后两条直线无限延长后必在这一侧相交。(注：在承认了公理 1)—4)的前提下，可推出"过给定直线外的一点，至少存在一条直线与给定直线不相交。")

而第五公理的一种等价的陈述为"过给定直线外的一点，至多存在一条直线与给定直线不相交。"

欧几里得在此基础上运用逻辑推断，导出了许许多多的命题(在

"几何原本"中包含了 465 个命题),从而构成了欧几里得几何学。自"几何原本"面世以来,人们就注意到欧几里得的第五公理(或称平行公理)是否与其他公理独立的问题,即平行公理能否用其他的公理推导出来。虽然很多学者(包括一些非常有名的数学家)曾宣称已证明了平行公理能用其他公理推导出来,但最后发现这些论证都是不正确的。于是从意大利数学家萨凯里(Saccheri,1733)开始,人们就转而猜测平行公理与其他的公理是独立的,即它不能从其他的公理推导出来。罗巴契夫斯基和 Bolya 分别在 1829 年和 1832 年独立地用平行公理的反命题,即用"过给定直线外一点,存在着至少两条直线与给定直线不相交"来替代平行公理,并由这套新的体系演绎出一套与欧氏几何迥然不同的命题,但却并没有导致任何矛盾,非欧几何就这样产生了。但是要让人们真正信服这种纯理性的几何体系,还是应该将这种"虚"的几何学真正地构造出来,也就是要提供这种"虚"几何的现实模型。在 19 世纪 70 年代,Klein 提出了 Klein 模型,等等。这些模型都能将非欧几何学在人们已经习惯的欧氏空间中实现。自此,非欧几何就成了一种"真正"的几何学。

长时期以来,人们已经知道欧几里得的几何体系存在着一些缺陷,如对一些基本概念(例如点、直线、平面)的定义存在着不清晰性,在某些命题的逻辑推断时无形中运用了欧几里得五个公理以外的"公理"等等。

1899 年 Hilbert 提出了欧氏几何的一套完整的公理体系。首先他提出了八个基本概念,其中三个是基本对象:{点、直线、平面};五个是基本关系:{点属于(或结合)直线,点属于(或结合)平面,一点在另两点之间,两线段合同,两角合同}。这些基本概念应服从下述五套公理:

结合公理(共有 8 个):

I_1. 对于两个不同的点,恒有一直线结合其中的每个点。

I_2. 对于两个不同的点,至多有一直线结合其中的每个点。

$I_{3.1}$. 每条直线上至少有两个不同的点。

$I_{3.2}$. 至少有三个不同的点不在一条直线上。

$I_{4.1}$. 对于不在一条直线上的三个点，恒有一平面通过它们中的每个点。

$I_{4.2}$. 每个平面至少有一个点。

I_5. 对于不在一直线的三个点，至多有一平面通过它们中的每个点。

I_6. 如果直线上的两个点在一个平面上，则此直线上的每个点都在这个平面上。

I_7. 如果两平面有一公共点，则至少还有另外一个公共点。

I_8. 至少有四点不在同一平面上。

顺序公理(共有 4 个)：

II_1. 若点 B 在点 A 和点 C 之间，则 A, B, C 是一直线上的不同三点，而且 B 也在 C 和 A 之间。

II_2. 对于任意两点 A 和 B，直线 AB 上至少有一点 C，使得 B 在 A 和 C 之间。

II_3. 在一直线上的任意三个点中，至多有一点在其余两点之间。

II_4. (Pasch(巴士)公理)　与一个三角形共面、但不过其顶点的直线，若与三角形的一边相交，则必与另一边相交。

合同公理(共有 5 个)：

III_1. 设 A, B 是直线 a 上的两点，A'是同一或另一直线 a' 上的一点，则在 a' 上点 A' 的已知一侧恒有一点 B'，使线段 AB 合同于线段 $A'B'$。记为 $AB \equiv A'B'$。

III_2. 若两线段(可以是相同的线段)都合同于第三线段，则这两个线段也合同。即

$$A'B' \equiv AB \quad A''B'' \equiv AB \Rightarrow A'B' \equiv A''B''。$$

III_3. 设开线段(AB), (BC)均在直线 a 上，而且没有公共点；开线段(AB), (BC), $(A'B')$, $(B'C')$均在同一或另一直线 a 上，亦无公共点。若 $AB \equiv A'B'$, $BC \equiv B'C'$，则 $AC \equiv A'C'$。

$III_{4.1}$. 已知平面 α 上的一角$\angle(h, k)$，指定平面 α' 上的一直线的一侧，以及这条直线上以点 O' 为原点的一条射线 h'，则 α' 上恰有一

射线k',使得$\angle(h, k)$合同于$\angle(h', k')$,且k'在α'的已知一侧。记为$\angle(h, k) \equiv \angle(h', k')$。

Ⅲ$_{4.2.}$ $\angle(h, k) \equiv \angle(k, h)$。

Ⅲ$_{5.}$(三角形合同公理) 对于两个三角形ABC和$A'B'C'$,若$AB \equiv A'B'$, $AC \equiv A'C'$, $\angle BAC \equiv \angle B'A'C'$, 则$\angle ABC \equiv \angle A'B'C'$。

连续公理:

Ⅳ.(Dedekind公理) 若线段AB两端及其内部的所有的点能被分为两类,具有下列性质:

① 每点恰属一类,A属于第一类,B属于第二类;

② 第一类中异于A的每个点在A和每个第二类点之间,则必存在一点C,使得A, C间的点都属于第一类,而C, B之间的点都属于第二类。称点C为Dedkind点或界点。由它所决定的分类叫做一个Dedkind分割。

平行公理:

(欧氏平行公理) 对于任何直线a和不在其上的任何点A,至多有一条直线过A,而且与直线a共面,但不相交。

从这些公理出发,根据逻辑推断所得出的一系列命题就构成了欧氏几何的全部内容。Hilbert并证明了:只要承认实数系统是相容的,则这套公理系统是相容的、独立的、完备的,其中

"相容性"是指:由这套公理系统不可能导出两个互相矛盾的命题。

"独立性"是指:公理系统中的任何一个公理都不能由其他公理推导出来。

"完备性"是指:这套公理系统所刻划的几何是唯一的,即不可能有两套不同的几何学,但它们都适合这套公理系统。

于是,自Hilbert以后,人们就能用一套严密的体系来描述欧几里得几何学。我们也可采用公理系统的方法去描述非欧几何,这只需将欧氏几何中的平行公理换成其逆命题。同样可证明:只要承认欧氏几何是相容的,则非欧几何也必是相容的、独立的和完

备的。我们可用 Poincaré 的上半平面模型作为例子来阐述非欧平面几何。在 Poincaré 的上半平面模型中，它的基本概念可作如下的理解：

“点”⇔上半(开)平面中的点。

“直线”⇔上半平面中与 x 轴垂直的直线，或上半平面中以 x 轴上的点为圆心的上半圆周。

“点 A 属于(或结合)直线 α”⇔上半平面中代表 A 的那一个点属于代表直线 α 的那条与 x 轴垂直的直线，或以 x 轴上的点为圆心的上半圆周。

“点 B 在另两点 A、C 之间”⇔A、B、C 三点属于上半平面中同一条与 x 轴垂直的直线，或属于上半平面中同一个以 x 轴上的点为圆心的上半圆周上，而且排列的次序是依次为 A、B、C。

“两线段合同”⇔利用一系列关于与 x 轴垂直的直线的对称，或关于以 x 轴上的点为圆心的半圆的反演后能将一线段变至另一线段。

“两角合同”⇔利用一系列关于与 x 轴垂直的直线的对称，或关于以 x 轴上的点为圆心的半圆的反演后能将一角变至另一角。

可以验证这些基本概念是服从结合公理、顺序公理、合同公理、连续公理所规定的约束，而且此模型满足非欧几何的“平行公理”，即“过给定直线外的一点，可作至少两条与给定直线不相交的直线。”

3. 微分几何学、黎曼几何学

大家知道笛卡儿在欧氏空间中引入了直角坐标系后，利用数形结合就形成了解析几何学。但是在解析几何学中一般只处理点、直线、平面、二次曲线、二次曲面等几何对象，这是因为将图形转化为数据以后，笛卡儿仅用初等代数学来处理这些数据。随着微积分的发展，分析学也进入了几何学，所以可以利用微积分来揭示出曲线、曲面在其一点附近的弯曲程度，这就形成了三维欧氏空间中曲线和曲

面的微分几何学。Gauss 在这方面有着杰出的贡献。曲面论的主要想法是把用参数(u, v)表示的曲面上两个无限邻近点之间的距离 ds 表示成 $ds^2 = Edu^2 + 2Fdudv + Gdv^2$，其中 E、F、G 都是参数 u、v 的函数。我们称矩阵

$$\begin{pmatrix} E & F \\ F & G \end{pmatrix}$$

为该曲面的度量矩阵，曲面上的许多弯曲的性质都可用度量矩阵刻划出来。

到了 1854 年，黎曼提出了现今人们称之为“黎曼几何学”的思想。在已采用了坐标系$\{x^1, \cdots, x^n\}$的 n 维空间中，他引入了无限邻近的两点$(x^1, \cdots, x^n)$和$(x^1 + dx^1, \cdots, x^n + dx^n)$之间的“距离”$ds$ 的概念，ds^2 可用 $dx^1, \cdots, dx^n$ 的一个正定二次型来表出：

$$ds^2 = \sum_{i,\ j=1}^{n} g_{ij}(x) dx^i dx^j$$

其中(g_{ij})是一个正定矩阵。

后来人们将这种带有度量 ds^2 的空间称为黎曼空间。欧氏几何是一种最简单的黎曼几何，这时的 $g_{ij} = \delta_{ij}$，即

$$ds^2 = (dx^1)^2 + \cdots + (dx^n)^2$$

利用度量 ds，我们可以导出黎曼空间中曲线的弧长、区域的面积、向量的平行移动等几何概念，并由此发展成一种崭新的几何学。后来 Minkowski，Lorentz 等人再将黎曼几何中度量正定性的限制去掉，即 $g_{ij}(x)$也可以不是正定的(但要求它是非退化的)，这样就导出了 Lorentz 几何，这时

$$ds^2 = \sum_{i,\ j=1}^{n} g_{ij}(x) dx^i dx^j$$

其中矩阵(g_{ij})是一个非正定的，但行列式不等于 0 的矩阵。特别地，当

$$
(g_{ij}) = \begin{pmatrix} +1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix}
$$

时，称这种 Lorentz 空间为 Minkowski 空间。

4. 四维时空、爱因斯坦狭义相对论、广义相对论

直至 19 世纪末，黎曼几何学或 Lorentz 几何学仍停留在纯理论的发展阶段。但到了 20 世纪初，局面有了明显的变化。大家知道，数学是一门研究现实世界中的数量关系和空间形式的科学。长时期以来，人们习惯地认为欧几里得空间是现实空间的一种最好的描述。牛顿就采用欧几里得空间来描述物体所在的空间。在牛顿力学中，时间是绝对的，时间和空间是两种类型截然不同的参量。如果在三维欧氏空间中选用笛卡儿直角坐标系$\{O;\ x,\ y,\ z\}$，则物体在时刻 t 的空间位置可用$(t,\ x,\ y,\ z)$来表示。如果将坐标系$\{O;\ x,\ y,\ z\}$沿 x 轴按常速 a 作平移运动（无转动），则运动坐标系$\{O';\ x',\ y',\ z'\}$与静止坐标系$\{O;\ x,\ y,\ z\}$之间的变换关系为

$$
\begin{cases} x' = x - at \\ y' = y \\ z' = z \end{cases}
$$

于是同一质点在这两个不同坐标系中所观察到的速度是不同的，质点在静止坐标系$\{O;\ x,\ y,\ z\}$中的速度向量 $\vec{v} = (v_x,\ v_y,\ v_z)$ 与在运动坐标系$\{O';\ x',\ y',\ z'\}$中的速度向量 $\vec{v'} = (v'_{x'},\ v'_{y'},\ v'_{z'})$ 之间有下面的关系：

$$
\begin{cases} v'_{x'} = \dfrac{\mathrm{d}x'}{\mathrm{d}t} = \dfrac{\mathrm{d}x}{\mathrm{d}t} - a = v_x - a \\ v'_{y'} = \dfrac{\mathrm{d}y'}{\mathrm{d}t} = \dfrac{\mathrm{d}y}{\mathrm{d}t} = v_y \\ v'_{z'} = \dfrac{\mathrm{d}z'}{\mathrm{d}t} = \dfrac{\mathrm{d}z}{\mathrm{d}t} = v_z \end{cases}
$$

但是从 19 世纪末所发现的著名的 Michelson 实验(1881)中知道,在这两个不同的惯性系下所测到的光速(即光子的速度)却总是相同的。这一个现象是很难用牛顿力学的理论去解释的。1905 年爱因斯坦提出了狭义相对论,他认为时间和空间应该融合在一起,成为四维时空。而称(t, x, y, z)为四维时空中的一个事件。爱因斯坦认为这个四维时空的几何学应该是 Minkowki 几何学,即两个无限邻近的事件(t, x, y, z)和$(t+dt, x+dx, y+dy, z+dz)$之间的"距离"(物理中称为"时空间隔")ds应满足

$$ds^2 = c^2dt^2 - dx^2 - dy^2 - dz^2$$

而两个惯性系之间的坐标变换应使无限邻近的两个事件之间的"时空间隔"保持不变。于是爱因斯坦推算出在 Minkowski 时空中,上述两个惯性系之间的坐标变换应该是

$$\begin{cases} x' = \dfrac{x - at}{\sqrt{1-\left(\dfrac{a}{c}\right)^2}} \\ y' = y \\ z' = z \\ t' = \dfrac{t - axc^2}{\sqrt{1-\left(\dfrac{a}{c}\right)^2}} \end{cases}$$

称这种变换为 Lorentz 变换。即它是使 Minkowski 几何学中的度量

$$ds^2 = c^2dt^2 - dx^2 - dy^2 - dz^2$$

保持不变的一种变换,即使得

$$c^2dt'^2 - dx'^2 - dy'^2 - dz'^2 = c^2dt^2 - dx^2 - dy^2 - dz^2$$

利用 Lorentz 变换,质点在坐标系$\{O; x, y, z\}$中的速度向量$(v_x, v_y, v_z) = \left(\dfrac{dx}{dt}, \dfrac{dy}{dt}, \dfrac{dz}{dt}\right)$与在坐标系$\{O'; x', y', z'\}$中的速度

向量

$$(v'_{x'},\ v'_{y'},\ v'_{z'}) = \left(\frac{\mathrm{d}x'}{\mathrm{d}t'},\ \frac{\mathrm{d}y'}{\mathrm{d}t'},\ \frac{\mathrm{d}z'}{\mathrm{d}t'}\right)$$

之间应有下述关系：

$$\begin{cases} v'_{x'} = \dfrac{v_x - a}{1 - v_x \dfrac{a}{c^2}} \\ v'_{y'} = \dfrac{v_y \sqrt{1 - \dfrac{a^2}{c^2}}}{1 - v_x \dfrac{a}{c^2}} \\ v'_{z'} = \dfrac{v_z \sqrt{1 - \dfrac{a^2}{c^2}}}{1 - v_x \dfrac{a}{c^2}} \end{cases}$$

特别地，如光子沿 x 轴以光速 c 运行，即

$$v_x = c,\ v_y = 0,\ v_z = 0$$

则由 Lorentz 变换所导出的速度变换公式得知，光子在惯性系 $\{O';\ x',\ y',\ z'\}$ 下的速度为

$$\begin{cases} v'_{x'} = \dfrac{c - a}{1 - \dfrac{a}{c}} = c \\ v'_{y'} = 0 \\ v'_{z'} = 0 \end{cases}$$

这样，爱因斯坦就圆满地解释了光速不变性。在此基础上，爱因斯坦得出了著名的质能公式 $E = mc^2$。

随着狭义相对论的巨大成功，爱因斯坦在 1916 年又提出了著名的广义相对论，用来解释引力的由来。他认为由于物质分布的存在，使得四维时空产生了弯曲，即这时的四维时空的几何学应该是

Lorentz 几何学，而光线运行的空间轨迹是由四维时空的 Lorentz 几何中的测地线(即短程线)对其三维空间部分的投影所确定的。而表征物质分布的能量动量张量 T_{ij} 与表征四维 Lorentz 时空弯曲程度的度量 g_{ij} 之间要满足著名的爱因斯坦场方程：

$$R_{ij}-\frac{R}{2}g_{ij}=T_{ij}$$

其中 R_{ij} 是由度量 g_{ij} 所确定的 Ricci 张量，R 是由 g_{ij} 所确定的数量曲率。

爱因斯坦场方程是一个关于度量 g_{ij} 的偏微分方程组。根据爱因斯坦场方程的一个特解——Schwarzschield 真空解，爱因斯坦提出了广义相对论的三大实验验证：水星近日点的进动，光线的重力偏转，引力偏移，从而确立了广义相对论的正确性。爱因斯坦广义相对论的成功极大地推动了黎曼几何学在 20 世纪的飞速发展。

第十节　费马大定理终于成为定理

1. 费马大定理的由来

费马(Pierre de Fermat, 1601—1665)是法国人，一位业余数学家。他是解析几何的创始人之一。1637 年左右，他在阅读丢番图的《算术》时，在页边用拉丁文写下了以下一段话："不可能把一个立方数分成两个立方数，或者把一个四方数分成两个四方数，而且一般说来，不可能把任何一个大于二次幂的方幂数分成两个同次幂的方幂数。""我对此找到了一个绝妙的证明，可惜这里空白太小，写不下。"表示成现代的语言就是："$x^n + y^n = z^n$, $xyz \neq 0$，当 $n > 2$ 时无整数解。"

这段话是在他死后才发现的，是费马留下的最后一个尚未证明的"定理"，因此英文中称为"费马最后定理"(Fermat's Last Theorem)，简称"FLT"。

(1) 勾股数

当 $n = 2$ 时，方程 $x^2 + y^2 = z^2$ 有无穷多组非零整数解。我们可用几何的方法加以解释。显然 $x^2 + y^2 = z^2$ 的整数解问题等价于 $X^2 + Y^2 = 1$ 的有理数解问题。而后一方程的实数解是平面上的单位圆，因此问题归结为单位圆上的有理点(坐标均为有理数的点)问题。

取圆上一点 $M(-1, 0)$，设 $P(X, Y)$是圆周上任意一点，则直线 MP 的斜率 $t = \dfrac{Y}{1+X}$ (见图 3.10.1)。反之，对于给定的斜率 t，一定可作一条直线 MP 与圆周交于 $P(X, Y)$，使 $Y = t(1+X)$。由

于 P 在圆周上，代入圆方程可解得

$$\begin{cases} X = \dfrac{1-t^2}{1+t^2} \\ Y = \dfrac{2t}{1+t^2} \end{cases}$$

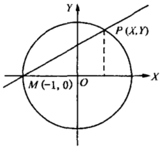


图 3.10.1

不难看出 $P(X, Y)$是圆周上有理点当且仅当 t 是有理数。因此圆周上除 $M(-1, 0)$外的有理点与全体有理数成一一对应。这也证明了 $x^2+y^2=z^2$ 有无穷多组整数解。

事实上只要令 $t=\dfrac{q}{p}$，p，q 是整数，就有

$$\begin{cases} x = p^2-q^2 \\ y = 2pq \\ z = p^2+q^2 \end{cases}$$

是 $x^2+y^2=z^2$ 的一组整数解。反过来有以下定理。

定理 方程 $x^2+y^2=z^2$ 的满足下列条件：

$$(x, y)=1,\ x>0,\ y>0,\ z>0,\ 2\mid x$$

的整数解可以表示成

$$\begin{cases} x = 2pq \\ y = p^2-q^2 \\ z = p^2+q^2 \end{cases}$$

其中 $p>q>0$，$(p, q)=1$，p，q 一奇一偶。

直角三角形的 3 条边长满足上述等式，因此方程 $x^2+y^2=z^2$ 的正整数解对应于边长为整数的直角三角形的 3 条边长。直角三角形边长的平方和关系相传是公元前 5 世纪的希腊数学家毕达哥拉斯(Pythagoras)首先发现，因此称为毕达哥拉斯定理，对应的 3 个整数称为毕达哥拉斯数。我国古代数学书《周髀算经》(约成书于公元前 1 世纪西汉时期)中曾经提到“勾广三，股修四，径隅五”这个三边都

是正整数的直角三角形，说明我们的祖先也早已知道直角三角形三边长度的关系。因此我国数学家称此定理为勾股定理，相应的一组数称为勾股数。

(2) 无限下降法

当 $n > 2$ 时，情况大不相同。费马断定 $x^n + y^n = z^n$ 当 $n > 2$ 时无非零整数解。但人们始终没有找到他的证明。可以肯定的是：费马用“无限下降法”证明了 $n = 4$ 的情形。还证明了更强的命题“$x^4 + y^4 = z^2$ 无非零整数解”。

设 $x^4 + y^4 = z^2$，其中 x、y、z 是两两互素的正整数，根据前面关于勾股数的定理，假设 x 是偶数，则必存在一奇一偶的一对正整数 $p > q > 1$，$(p, q) = 1$，使得

$$x^2 = 2pq,\ y^2 = p^2 - q^2,\ z = p^2 + q^2$$

于是 $y^2 + q^2 = p^2$ 由于 p 一定是奇数，因此 q 是偶数，再次应用定理，我们又能得到 $q = 2ab$，$y = a^2 - b^2$，$p = a^2 + b^2$，其中 $a > b > 0$，$(a, b) = 1$，a，b 一奇一偶。因此 $x^2 = 4ab(a^2 + b^2)$。说明 $ab(a^2 + b^2)$ 是平方数。但因 $(a, b) = 1$，可得$(ab, a^2 + b^2) = 1$，因而 ab 与 $p = a^2 + b^2$ 都是平方数，从而 a，b 也是平方数。令 $a = \bar{x}^2$，$b = \bar{y}^2$，$p = \bar{z}^2$，我们得到

$$\bar{x}^4 + \bar{y}^4 = \bar{z}^2$$

显然有 $\bar{z} < \bar{z}^2 = p < p^2 + q^2 = z$，这说明 $x^4 + y^4 = z^2$ 的非零正整数解中的 z 可以不断减小，与正整数集合的性质相悖。这正是“无限下降法”名称的来由。

2. 欧拉对 $n = 3$ 的证明

在费马之后的第一个突破无疑属于伟大的数学家欧拉(L. Euler, 1707—1783)。他应用无限下降法证明了 $n = 3$ 的情形。下面就是他的证明。

假设 $x^3+y^3=z^3$ 有非零正整数解。在除去它们的公因子后，不妨设 $(x, y, z)=1$。由于 x、y、z 中任意两个数的公因子一定整除第三个数，因此 x、y、z 一定两两互素，而且这三个数中必有一个而且只有一个是偶数。

设 x、y 是奇数，z 是偶数，则 $x+y$, $x-y$ 均为偶数。于是可设

$$x+y=2p,\ x-y=2q$$

从而

$$x=p+q,\ y=p-q$$

$$z^3=x^3+y^3=(x+y)(x^2-xy+y^2)=2p(p^2+3q^2)$$

由于 x, y 是互素的奇数，因此 p、q 也互素，且奇偶性不同。又若 $q=0$ 时，$x=y=1$ 不是方程的解，因此 p、q 均不等于 0，而且必要时交换 x、y 的次序，可设 p、$q>0$。

先考虑 $3\nmid p$ 的情形。此时由 $(p, q)=1$, $(p, 3)=1$, 可以推出 $(2p, p^2+3q^2)=1$（注意到 p、q 奇偶性不同，因此 p^2+3q^2 是奇数）。而已知 $2p(p^2+3q^2)=z^3$ 是一个立方数，因此 $2p$ 和 p^2+3q^2 都是立方数。由于

$$(a^2+3b^2)^3=(a^3-9ab^2)^3+3(3a^2b-3b^3)^2$$

因此若能找到整数 a、b 使得

$$p=a^3-9ab^2,\ q=3a^2b-3b^3$$

那么 p^2+3q^2 一定是立方数。可是反过来是否正确呢？即若 p^2+3q^2 是一个立方数，是否一定存在 a、b 满足上述等式？这是欧拉证明的关键。当欧拉于 1753 年宣称他能证明费马大定理的 $n=3$ 的情形时，他在这一点上的证明是错误的。可是从他以后的工作中可以导出一个正确的证明。因此人们认为欧拉于 1770 年证明了 $n=3$ 的情形。这个关键的证明与唯一因式分解有关。我们把它略去了。

现在我们假设存在整数 a、b，使得

$$p = a^3 - 9ab^2 = a(a-3b)(a+3b)$$

$$q = 3a^2b - 3b^3 = 3b(a-b)(a+b)$$

那么由 p、q 互素一定能得出 a、b 互素，由 p、q 奇偶性不同可知 a、b 的奇偶性也不同。此外，$2p = 2a(a-3b)(a+3b) =$ 立方数，由于 $a \pm 3b$ 是奇数，因此

$$(2a,\ a \pm 3b) = (a,\ a \pm 3b) = (a,\ \pm 3b) = (a,\ 3)$$

由假设，$3 \nmid p$ 可得 $(a,\ 3) = 1$。因此 $(2a,\ a \pm 3b)$ 互素，而 $a+3b$ 与 $a-3b$ 的公因子一定是 a 与 $3b$ 的公因子。所以 $a+3b$，$a-3b$ 也互素，于是 $2a$，$a-3b$，$a+3b$ 是两两互素的。从而这三个数都必须是立方数。不妨设

$$2a = s^3,\ a - 3b = t^3,\ a + 3b = u^3$$

即有 $u^3 + t^3 = s^3$。我们又得到了 $x^3 + y^3 = z^3$ 的一组新解 $(u,\ t,\ s)$，它满足 $s^3t^3u^3 = 2p < 2p(p^2 + 3q^2) = z^3$。因此，$s$、$t$、$u$ 的绝对值均小于 z。问题是 $(u,\ t,\ s)$ 不一定全是正整数。但若 $u < 0$ 时，我们可把原等式化为 $s^3 + (-u)^3 = t^3$。用类似的方法，我们总可以得到一组正整数解，使得 $s < z$。这样就能应用"无限下降法"了。

对 $3 \mid p$ 的情形，可设 $p = 3v$，则

$$2p(p^2 + 3q^2) = 3^2 \cdot 2v(3v^2 + q^2)。$$

由于 $3 \nmid p$，因此 $3^2 \cdot 2v$ 和 $3v^2 + q^2$ 互素，从而它们都是立方数。用与前类似的论证，即可应用"无限下降法"。

3. 索菲·热尔曼的贡献

法国女数学家索菲·热尔曼(Sophis Germain, 1776—1831)于1820年证明了以下定理：

若 p 是素数，$2p+1$ 也是素数，则 $x^p + y^p = z^p$ 没有使 p 不能整除 x、y、z 之一的解。这种素数称为第一类的，否则是第二类的素

数。可以证明对于第一类的素数，当 $n \leqslant 100$ 时费马大定理正确。这是第一个对一批素数证明费马大定理的结论。受她的证明的影响，$n=5$ 的情形于 1825 分别由狄利克雷和勒让德证明，$n=7$ 的情形于 1839 年被拉梅证明。

到 19 世纪 40 年代时，人们想到应用复数来证明费马大定理。因为很容易看出，如果对于一个素数 p 能证明费马大定理，那么对于任何含有素数因子 p 的正整数 n，费马大定理也成立。因此只需对奇素数 p 证明费马大定理就够了。

设有两两互素的正整数 x、y、z 是方程 $x^p+y^p=z^p$ 的解，则在复数域里有分解式：

$$x^p+y^p=(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y)=z^p \qquad ①$$

其中 $\zeta=\cos\frac{2\pi}{p}+\mathrm{i}\sin\frac{2\pi}{p}$ 是单位原根。因式分解式①的系数都在代数整数环 $\mathbb{Z}[\zeta]=\{a+b\zeta \mid a、b\in\mathbb{Z}\}$ 内。如果其中任意两个因子有素数公因子 q，则由 $q \mid x+\zeta^i y$，$q \mid x+\zeta^j y$，可以得到

$$q \mid (x+\zeta^i y)-(x+\zeta^j y)=\zeta^i y(1-\zeta^{j-i})=\zeta^i\cdot\frac{1-\zeta^{j-i}}{1-\zeta}\cdot y(1-\zeta)$$

又 ζ^i 与 $\frac{1-\zeta^{j-i}}{1-\zeta}$ 都是环 $\mathbb{Z}[\zeta]$ 中的乘法可逆元，故 $q \mid y(1-\zeta)$。

类似地，由

$$\begin{aligned} q \mid \zeta^j(x+\zeta^i y)-\zeta^i(x+\zeta^j y) &= -\zeta^i x(1-\zeta^{j-i}) \\ &= -\zeta^i\cdot\frac{1-\zeta^{j-i}}{1-\zeta}\cdot x(1-\zeta) \end{aligned}$$

可得 $q \mid x(1-\zeta)$。

考虑到 x、y 互素，即有 $q \mid 1-\zeta$。这证明了分解式①的任意两个因子的公因子必是所有因子的公因子。

当时人们认为在这个代数整数环中有唯一因式分解。如果分解式①中的任意两个因子都互素，那么每个因子都应是一个 p 次幂，从而有可能用无限下降法导出矛盾。如果其中有两个因子不互素，

则可以导出这 p 个因子有公因子。又能用无限下降法导出矛盾。可是库默尔的发现粉碎了这个希望。

德国数学家库默尔(Ernst Eduard Kummer, 1810—1893)在试图证明费马大定理时发现在一般代数整数环中唯一因子分解定理不成立。例如在 $a+b\sqrt{-5}$ 构成的代数整数环中,有两个不同的素因子分解: $6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$。库默尔引进了理想数的概念,在他所研究的整数环中,存在着理想数的唯一因子分解定理。他利用理想数证明了费马大定理在一些情况下是正确的。

库默尔证明了如果对于奇素数 p、p 不能除尽代数数域 $\mathbb{Q}(\zeta)=\{a+b\zeta \mid a, b\in\mathbb{Q}\}$ 的类数 h_p,则费马方程 $x^p+y^p=z^p$ 没有有理整数解(x, y, z)使得 $p\nmid xyz\neq 0$。

在 100 以内的素数中,除了 37, 59, 67 以外,其余奇素数都满足上述定理的条件。从而对于这些奇素数费马定理均成立。根据这个理论,通过计算机的计算,可以证明对于小于 400 万的奇素数,费马大定理都是正确的。

库默尔虽然没有能证明费马大定理,但是他开创了一个新的数学分支——代数数论。抽象代数中的"理想"就是来源于"理想数"。

4. 怀尔斯最终证明了费马大定理

1993 年 6 月 23 日,在英国剑桥的牛顿研究所的讲台上,英国出生的数学家安德鲁·怀尔斯(Andrew Wiles)宣布了一个震惊世界的消息:作为他所证明的定理的一个推论,费马大定理被证明了!虽然以后发现他的证明中有一个漏洞,但是大家还是相信这个漏洞是可以解决的。不过补漏还是花了将近两年的功夫。到 1995 年才发表在数学期刊《Annals of Mathematics》上。

怀尔斯实际上证明了半稳定的谷山—志村猜测:$\mathbb{Q}$ 上每条半稳定椭圆曲线均为模曲线。而如果费马方程有解 $a^p+b^p=c^p$,其中 a、b 互素,那么里贝特(Ribet)已经证明,由方程

$$y^2 = x(x+a^p)(x-b^p)$$

所确定的椭圆曲线不是模曲线。怀尔斯则根据半稳定的谷山—志村猜测证明了当整数 A、B 互素，且 $16 \mid AB(A-B)$ 时，椭圆曲线

$$y^2 = x(x+A)(x+B)$$

是模曲线。

取 $A = a^p$，$B = -b^p$，则

$$AB(A-B) = -a^p b^p (a^p + b^p) = -a^p b^p c^p$$

a、b、c 中必有一个偶数，因此当 $p > 3$ 时 $2^4 \mid AB(A-B)$。由此得到矛盾。费马大定理就得证了。

5. 椭 圆 曲 线

以下我们将简单地介绍一下怀尔斯证明的背景及基本思路。首先介绍什么是椭圆曲线以及模曲线。

假设取定了一个虚部大于 0 的复数 τ，集合

$$\Lambda = \{a + b\tau \mid a、b \in \mathbb{Z}\}$$

构成了复数平面上的一个格。以 0，1，τ，$1+\tau$ 为顶点的平行四边形 T 称为格 Λ 的基本区域(见图 3.10.2)。任意一个复数都可以表示成 $z+(a+b\tau)$ 的形式，其中 $z \in T$，$a+b\tau \in \Lambda$。当 z 不在 T 的边界上时，z 是唯一确定的，而当 z 落在 T 的边界上时，z 不唯一，例

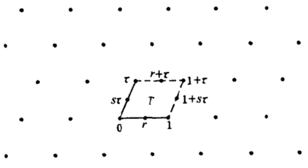


图 3.10.2

如当 $0<r,\ s<1$ 时,有

$$r+(a+b\tau)=r+\tau+(a+(b-1)\tau)$$

$$s\tau+(a+b\tau)=1+s\tau+((a-1)+b\tau)$$

也就是说 T 的下边上的点 r 与上边的点 $r+\tau$ 有一个等价关系,左边的点 $s\tau$ 与右边的点 $1+s\tau$ 也有一个等价关系。此外,由于

$$\begin{aligned}0+(a+b\tau)&=1+((a-1)+b\tau)=\tau+(a+(b-1)\tau)\\&=1+\tau+((a-1)+(b-1)\tau),\end{aligned}$$

所以 T 的 4 个顶点都是等价的。因此我们重新定义基本区域为

$$T=\{z=x+y\tau \mid x,\ y\in\mathbb{R},\ 0\leqslant x,\ y<1\}$$

这样任意的复数都可以唯一地表示成 $z+(a+b\tau)$, $z\in T$ 的形式。

在复数平面上有一个亚纯函数

$$p(z)=\frac{1}{z^2}+\sum_{w\in\Lambda-\{0\}}\left(\frac{1}{(z-w)^2}-\frac{1}{w^2}\right)$$

称为魏尔斯特拉斯椭圆函数。这里要说一下椭圆函数名称的来历。

17 世纪时为了计算椭圆的弧长,得到了一些积分函数,这些积分不能用初等函数来表示,被称为椭圆积分。椭圆积分的反函数称为椭圆函数。因此椭圆函数可以理解为以椭圆的弧长作为自变量的函数,正如正弦和余弦函数是圆的弧长(以弧度来度量)的函数一样。圆的三角函数都是周期函数,椭圆函数也是周期函数,而且它有两个周期,后来就把双周期的亚纯函数统称为椭圆函数。

不难验证:

$$p(z+1)=p(z),\ p(z+\tau)=p(z)$$

说明魏尔斯特拉斯椭圆函数有两个周期 1 与 τ。更一般地,

$$p(z+(a+b\tau))=p(z),\ \forall a,\ b\in\mathbb{Z}$$

这表明只要知道 $p(z)$ 在基本区域 T 上的值,就能确定整个函数。魏

尔斯特拉斯函数的导函数

$$p'(z)=\sum_{w\in\Lambda}\frac{-2}{(z-w)^3}$$

也是一个双周期函数,所以也是椭圆函数。这两个函数有以下的关系式

$$(p')^2=4p^3-g_2p-g_3$$

其中

$$g_2=60\sum_{w\in\Lambda-\{0\}}\frac{1}{w^4},\ g_3=140\sum_{w\in\Lambda-\{0\}}\frac{1}{w^6}$$

利用魏尔斯特拉斯的两个椭圆函数可以定义从基本区域 $T-\{0\}$ 到复仿射平面$\mathbb{C}^2$内的一个映射:

$$\begin{aligned}\phi:\ T-\{0\}\ &\rightarrow\ \mathbb{C}^2\\ z\ &\rightarrow\ (p(z),\ p'(z))\end{aligned}$$

$\phi(z)$的坐标满足方程 $y^2=4x^3-g_2x-g_3$,因此$\phi(z)$是这个方程式所确定的 3 次代数曲线上的一个点。这里的$\mathbb{C}^2$是实欧氏平面的推广,称为复仿射平面。注意到 0 还没有对应点,因此有必要给仿射平面添加一条"无穷远直线"使其成为射影平面,记为$\mathbb{P}^2$。仿射平面内由 3 次多项式定义的曲线称为 3 次仿射代数曲线,这条曲线在射影平面里的闭包(就是把这条仿射曲线向无穷远处延伸所得到的无穷远直线上的点添加进去)称为相应的射影代数曲线,记为 C(见图 3.10.3)。我们这里的 3 次射影曲线 C 与无穷远直线只有一个交点,根据连续性原理,可以把 $\phi(0)$定义为这个无穷远点。这样就得到了一个映射

$$\phi:\ T\rightarrow C$$

这个映射是一一的,双向连续的。此外,这个 3 次多项式在曲线 C 的每一个点上至少有一个偏导数不等于 0,或者说曲线 C 的每一个点上都有一条切线。这样的曲线称为光滑的。这条光滑射影代数

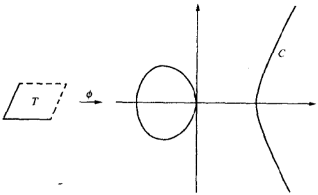


图 3.10.3

曲线称为椭圆曲线。反过来,对于任意的一条 3 次光滑射影代数曲线 C,总有一个虚部大于 0 的复数 τ,使得由 1 与 τ 确定的基本区域 T 可以用上面定义的方式一一地映到曲线 C 上。因此可把椭圆曲线定义为复射影平面$\mathbb{P}^2$上的光滑 3 次曲线。

从上面的介绍可以知道,椭圆曲线与椭圆之间只有极其遥远的亲缘关系。两者的性质截然不同。不要把椭圆曲线与椭圆相混淆。

读者还要注意的是:现在我们是在复数范围里讨论问题,复数本身是 2 维的,复的仿射平面就是 4 维的空间,已经无法在现实世界里实现了。而一个复数变量的多项式等于 0,则可以等价于实部与虚部分别等于 0 的两个方程式,因此一条代数曲线相当于 4 维空间里由两个方程所确定的零点集,应该是一个 2 维的点集。也就是通常所说的曲面。这就是为什么代数曲线也被称为黎曼面的原因。通过上面定义的 ϕ,椭圆曲线的直观形象就是复数平面内的一个基本区域 T。

为了赋予 T 一个更合适的形象,我们首先通过连续的等价拓扑变换将其变形成一个矩形,由于矩形下边的点等价于上边的对应点,因此把对应点粘合,就得到一个圆筒。圆筒两端的圆周就是原矩形的左边与右边。再把它们的对应点粘合,最终得到一个车胎面,或者说一个油炸面包圈,也被称为环面(torus)(见图 3.10.4)。这就是数学家心目中的椭圆曲线的形象。顺便说一下,任何一条光滑射影代

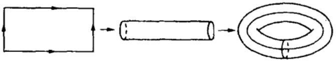


图 3.10.4

数曲线都可以通过可逆拓扑变换变形成一个多孔油饼面的模样(见图 3.10.5),其中孔的个数 g 是代数曲线的一个最重要的不变量,称为亏格。椭圆曲线的亏格等于 1。代数曲线的亏格愈大,其构造愈复杂。



图 3.10.5

最后再说几句关于有理曲线的话。在讨论勾股数时,我们已经为单位圆建立了一个有理函数的参数方程,如果推广到复数域上,很容易看出这个参数方程组在除去$\pm$i 的复数集合 $\mathbb{C}-\{i, -i\}$ 与去掉一个点 $M(-1, 0)$的单位圆周间建立了一个一一对应。全体复数的集合$\mathbb{C}$ 可以看成一条复仿射直线,添加一个无穷远点后就成为复射影直线$\mathbb{P}^1$。而在参数方程组中如果让 t 趋向无穷大,则点(X, Y)的极限是$(-1, 0)$,可见令$\mathbb{P}^1$的无穷远点对应到 $M(-1, 0)$点是合理的。而 i 与$-$i 则分别对应到复的单位圆周与射影平面的无穷远直线的两个交点。这样就建立了射影直线$\mathbb{P}^1$与复射影平面内的单位圆周间的一一对应。凡是能与射影直线一一对应的射影代数曲线称为有理曲线。其实复射影平面内的 1 次与 2 次光滑代数曲线都是有理曲线。因此椭圆也是一条有理曲线。从有理曲线的构造可以看出,它只要有一个有理点,就一定有无限多个有理点。而椭圆曲线则不同,它上面的有理点构成一个有限生成的交换群。至于亏格大于 1 的曲线则只有有限多个有理点,这就是著名的莫德尔(Mordell)猜测,于 1983 年才被法尔廷斯(Faltings)证明,后者并因此而获得了菲尔兹奖。由于 d 次光滑代数曲线的亏格等于 $\frac{1}{2}(d-1)(d-2)$,因

此由方程 $X^n+Y^n=1$ 定义的费马曲线(这是一条光滑曲线)的亏格当 $n\geqslant 4$ 时的亏格一定大于1,从而最多只有有限多个有理解。由此可见代数方程的有理点问题还有着深刻的几何含义。

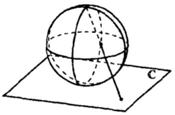


图 3.10.6

我们看一下射影直线的几何形象。通过左图所示的球极投影可使复数平面 $\mathbb{C}$ 上的所有点与球面上除北极外的所有点成一一对应,球面的北极恰好对应于无穷远点,因此球面就与射影直线 $\mathbb{P}^1$ 成一一对应(见图 3.10.6)。可见 $\mathbb{P}^1$ 几何形象是一个球面,它的亏格等于0。与用 $d=1$、2 代入亏格公式算得的结果相同。有理曲线确实是最简单的代数曲线。

从上一节的讨论可以知道,每一条椭圆曲线都能对应一个虚部大于0的复数 τ,使得由1与 τ 生成的基本区域 T 能与这条椭圆曲线对应。但是同一条椭圆曲线对应的 τ 不唯一,例如1与 $1+\tau$ 生成的平行四边形也是一个基本区域。可以证明两个具有正虚部的复数 τ 与 τ' 确定同一条椭圆曲线的充分必要条件是它们之间有以下关系:

$$\tau'=\frac{a\tau+b}{c\tau+d},\ a,\ b,\ c,\ d\in\mathbb{Z},\ ad-bc=1 \qquad ②$$

我们称 τ 与 τ' 等价。

又因具有正虚部的复数就是位于上半复数平面(以下记为 H)的复数,因此我们可以对上半平面的复数加以分类,并得到关于上述等价关系的一个基本区域 Ω,如图3.10.7所示。

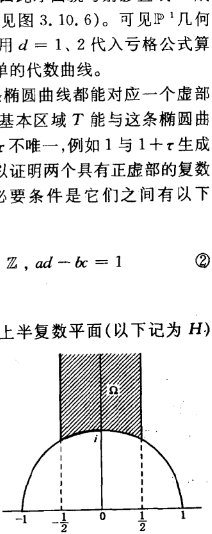


图 3.10.7

这里的基本区域 Ω 是图中的阴影部分,包括左半部分用粗线画出的边界,但不包括右半部分用细线画出的边界。基本区域的含义是对

任何一条椭圆曲线都能在基本区域内找到唯一的一个与之对应的 τ。再来看看这个基本区域 Ω 的几何形象：如果把左右两半边界的对应点粘合起来，我们得到一个化学实验用的无限长的试管，假如再添上一个无穷远点使这个试管封闭(数学家称之为"紧化")，则又得到一个球面，也就是射影直线 $\mathbb{P}^1$！如果把 Ω 的紧化记为 $\overline{\Omega}$，则有 $\overline{\Omega} \cong \mathbb{P}^1$。也就是说基本区域的紧化是一条代数曲线。这样的代数曲线称为模曲线。

②式定义的等价关系可以推广为

$$\tau' \sim N^{\tau} \Leftrightarrow \tau' = \frac{a\tau + b}{c\tau + d}$$

$$a、b、c、d \in \mathbb{Z},\ ad - bc = 1,\ N \mid c$$

这里的 N 是一个正整数。这个等价关系也有一个基本区域 Ω_N，把这个基本区域紧化后也能得到一条代数曲线 $X_0(N) = \overline{\Omega}_N$，这种曲线也称为模曲线。如果 E 是一条定义在有理数域上的椭圆曲线，并且存在一条模曲线 $X_0(N)$ 以及满足某些条件的映射 $X_0(N) \to E$，则也称 E 是模曲线。例如椭圆曲线 $y^2 = x(x+3^2)(x-4^2)$ 就是对应于 $X_0(15)$ 的模曲线。著名的谷山—志村猜测认为所有椭圆曲线都是模曲线。

与模曲线有密切联系的一种函数称为模形式。模形式是定义在上半复数平面 H 上的一个解析函数 $f(z)$，它具有以下性质：

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^m f(z)$$

$$\forall\, a、b、c、d \in \mathbf{Z},\ ad - bc = 1,\ z \in H \qquad ③$$

其中 m 是由 f 确定的某个非负整数，称为 f 的权。比较②式与③式，就能看到它们之间的联系。

谷山—志村猜测是在 50 年代时由两位年轻的日本数学家谷山丰和志村五郎提出来的。开始时并没有引起太多人的注意。直至 1984 年一位年轻的德国数学家弗赖(G. Frey)提出了一个新的想法：

如果费马的方程有解 $A^n+B^n=C^n$, $n>2$, 那么由方程 $y^2=x^3+(A^n-B^n)x^2-A^nB^n$ 定义的椭圆曲线一定不是模曲线。因此只要谷山—志村猜测得到证明,费马大定理也就成立了。虽然弗赖当时提出的证明是错误的,但是在 1986 年里贝特补出了这个证明。现在很清楚了,为证费马大定理,只要证谷山—志村猜测就可以了。但是有谁知道这两个猜测中的哪一个更容易一些? 因此几乎没有人相信谷山—志村猜测会在短期内得到证明。只有唯一的例外,就是怀尔斯,他相信他有办法从谷山—志村猜测着手来证明费马大定理。

6. 怀尔斯证明的曲折过程

为了证明椭圆曲线都是模曲线,需要证明椭圆曲线的集合与模形式的集合间有着对应的关系。怀尔斯首先想到利用伽罗瓦(Galois)表示建立与模形式间的一一对应关系。为了这一步,他花费了 3 年。下一步的想法是建立某种计数理论,以说明两个集合有相同数量的元素。他首先想到的是岩泽(Iwasawa)理论,但是后来他听说弗拉赫(Flach)利用科利瓦金(Kolyvagin)的方法得到了一些类数公式,这真是他所需要的公式。于是他放弃了岩泽理论这条路,专注于弗拉赫—科利瓦金道路,直至 1993 年 6 月,他确信自己已经证明了谷山—志村猜测,于是在英国剑桥的牛顿研究所的讲台上,他宣布了这个震惊世界的消息:费马大定理被证明了!

可是在以后严格的审稿过程中,发现了其中的一个漏洞,它隐藏在弗拉赫—科利瓦金方法的内部。经过长时间的思考后,怀尔斯还是无法填补这个漏洞。他不得不重新回到原先给他放弃的岩泽理论,终于他发现利用某些黑克代数的环论性质可以帮他解决问题,最终得到正确的证明。这时已经到了 1994 年的秋季。他的论文则发表于 1995 年。

怀尔斯的证明绝对不可能是费马当年的证明(如果确实存在的话),因为怀尔斯的证明汇集了 20 世纪数论中所有的突破性工作,并把它们融合在一起。他创造了全新的数学技术,并将它们和传统的

技术以人们从未考虑过的方式结合起来。通过这样的做法，他开辟了处理为数众多的其他问题的新思路。这个证明是现代数学的完美综合，并将对未来产生不可估量的影响。有谁能想到一个小学生都能听懂的问题会蕴含如此深奥的原理，并要用到最现代化的数学工具才能最终解决呢？这也真是数学的魅力所在。

参考文献

[1] 西蒙·辛格. 费马大定理——一个困惑了世间智者 358 年的谜. 上海译文出版社，1998 年.

[2] Edwards. H. M. , Fermat's Last Theorem. Springer-Verlag, 1977.

[3] Wiles, A, Modular elliptic curves and Fermat's Last Theorem, Annals of Mathematics, 142(1995), 443—551.